PERSEREC

Technical Report 05-13
September 2005

Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations

Eric D. Shaw
Consulting & Clinical Psychology, Ltd.

Lynn F. Fischer
Defense Personnel Security Research Center

Research Conducted by
Defense Personnel Security Research Center

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders Analysis and Observations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**65**	

Technical Report 05-13 **September 2005**

Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders

Analysis and Observations

Eric D. Shaw
Consulting & Clinical Psychology, Ltd.

Lynn F. Fischer
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

Preface

This report provides an overview and analysis of 10 insider events that occurred prior to 2003 in infrastructure industries. It concludes with a set of observations that have clear implications for policies and management practices in government and industry. The 10 full case studies, authored by Eric D. Shaw, Ph.D., Consulting & Clinical Psychology, Ltd., are contained in another report that was issued as For Official Use Only in order to respect the confidentiality of private sector companies that were victimized by the offenders. These cases represent attacks against information systems that are essential for the functioning of national critical infrastructure industries.

The threat to organizations in this category is obviously a Department of Defense (DoD) concern; however, insider attacks, not unlike those described here, have also occurred in military departments and Defense agencies. PERSEREC has been tracking events on the government side over the past 3 years and has a growing database of information on trust betrayal involving information systems. A subsequent summary of findings that pertain specifically to the Defense community will be issued at a later date. In the interim, case study work of the type and quality seen here is proving to be invaluable to our understanding of this behavior and of mitigating factors that we would recommend to minimize Defense systems vulnerabilities.

The significance of the analysis of these events extends beyond a concern with the vulnerability of critical information technology (IT) systems. This is an attempt to understand one manifestation of the much larger insider threat to the DoD and the United States. Other dimensions of this threat include insider espionage—concerning which PERSERC has had a long-term research interest—and the insider threat associated with international terrorism that is only now emerging. These threats all stem from human problems and vulnerabilities that might be addressed in time to prevent damage or loss by an effective personnel security system working in harmony with employee assistance programs. For this reason, we are particularly interested in implications that focus on pre-employment screening, monitoring on the job, and on how to deal with otherwise valuable personnel who are angry or disgruntled.

James A. Riedel
Director

Executive Summary

This report offers an overview and analysis of 10 significant cases of trust betrayal. The cases in question were information technology (IT) insider events in which an insider or former insider, having had legitimate access to a critical information system, abused or violated that trust for personal advantage or to exact revenge on a person or organization. In each case the actions of a disgruntled or self-interested offender seriously damaged or compromised the operability of a critical information system. Also included in this report is a discussion of common themes and patterns emerging from the examination of these incidents under five general headings corresponding to clusters of significant issues or lessons emerging from the substance of the case narratives. These issue areas are: Subject and Attack Characteristics, Screening, Attack Detection, Organizational and Social Environment, and Personnel Management Issues.

The 10 cases of insider abuse involved offenders working in one of the critical sectors of the national infrastructure. The full narrative discussion of each of these cases is available in a companion report available to government personnel on request to the Defense Personnel Security Research Center (PERSEREC). Each case study discusses the offender's background, the organizational environment in which the offense took place, the details of each event, the offender's presumed motivations, final legal and investigative actions that resulted from the offense or attack, and lessons learned from each incident having implications for corporate policy or national security.

The threat to critical national infrastructure is obviously a Department of Defense (DoD) concern; and from our examination of cases in military departments and Defense agencies we see striking similarities with regard to situational factors, modus operandi, and motivations of offenders. Case studies on insider events that occur in the private sector can provide understanding of the value of deterrents and countermeasures that we might recommend to prevent this type of behavior in Defense organizations.

This study is also an attempt to understand one manifestation of the much larger insider threat to the DoD and to the federal government to include insider espionage and the emerging insider threat associated with international terrorism. What these threats have in common is that in most of these cases damage could have been prevented by timely and effective action to address the anger, pain, anxiety, or psychological impairment of perpetrators who exhibited signs of vulnerability or risk well in advance of the crime of abuse. Previous studies by PERSEREC indicate that much can be gained from a closer working relationship between the personnel security system and employee assistance programs. In the present study of IT insider offenders, we believe that the greater value of this effort is found in the lessons learned or implications that focus on pre-employment vetting, monitoring on the job, and on how to deal with personnel who are disgruntled or undergoing unusual stress.

This overview is followed by an assessment of whether, or to what extent, typologies, hypotheses, and predictive factors proposed earlier in published work by ourselves and other researchers are supported by the data derived from the present

research effort. We found that earlier work on critical pathway analysis, combined with the identification of at-risk characteristics, has strong potential for understanding why in these particular cases disgruntlement and other attitudinal characteristics led to significant damage or system compromise. Additional understanding can be gained from a characterization of individual insider offenders as belonging to one of several perpetrator subtypes identified in previous research. The offenders described in these case studies are by their motivations and behaviors easily recognized as falling into one of three subtypes described in earlier work by the primary author. In this group, there are four Proprietors, four Hackers, and two Avengers. We suggest that with additional inquiry it may be possible to link variations in critical paths to an insider attack with different perpetrator subtypes.

While specific findings and implications are found in the body of this report, we offer eight general observations that have clear application to cases like those described here for personnel policy, personnel security practices, technical deterrents, and security education for employee populations.

1. There is a strong relationship between personal stress as well as adverse social climates and the level of risk for systems abuse in any organization that relies heavily on information systems for production or mission requirements. Reliance on software solutions or technical deterrents to cyber-crime tends to obscure the importance of addressing personal issues through effective management interventions and timely referrals to employee assistance programs when appropriate.

2. Most of the offenders in these case studies were disgruntled for one reason or another. They reacted to their perceptions of injustice by abusive online behavior. An employee who is expressing anger in the workplace, is engaged in conflict with other employees, or otherwise is behaving in a threatening manner needs immediate management intervention. Our cases, albeit limited in number, indicate that there is a time delay in management awareness of employee disgruntlement and, therefore, a window of opportunity for more prompt and effective management responsiveness to this challenge.

3. Even where disgruntlement or stress were not factors, these cases indicate that an elevated vulnerability to abuse exists in organizations that permit systems administrators or other IT professionals exclusive or proprietary control over their information systems. Where the system administrator has a sense of ownership and possesses technical skills not shared by other members of the organization, management has no supervisory oversight and may well be intimidated by the administrator. The solution to this vulnerability is to require some type of routine system audit or monitoring by an independent provider or shared responsibilities for IT functions within the organization by technically qualified persons.

4. Inadequate termination policies appear to have been a contributing factor in the majority of cases studied here and in other insider events evaluated by the research team. Where termination of employment or temporary probation appears to be a

necessary action in extreme cases, the organization must protect itself and its systems from acts of retribution. Immediate assessment and suspension of an individual's full access (remote and onsite) as well as physical access to the workplace by a terminated employee may be warranted, particularly when that employee has had some level of functional control of the IT system.

5. While remote access to a critical information system can be justified as a convenience or as a necessity stemming from mission requirements, experience indicates that unmonitored remote access carries intensified risks to an IT system. System vulnerability is heightened by not suspending remote access privileges of an employee who is barred from the workplace, known to be disgruntled, or who has a history of disregarding security rules and procedures.

6. Some of the system abuse reported in these cases would not have occurred had there been effective pre-employment screening of job applicants, particularly in regard to past history of online and criminal behavior. Employers, whether in government or the private sector, face serious risks by hiring IT professionals based simply on personal recommendation or paper credentials.

7. A review of the recent history of insider cyber-crime and abuse shows that some of these damaging events could have been avoided by adequate security training, education, and awareness for employees having access to, or control over, critical information systems. Educational and awareness programs for the workforce and the timing of awareness communications may be geared to activate during periods of higher vulnerability for the organization or during a window of opportunity after signs of employee disgruntlement surface.

8. In some of these cases, the failure to alert management to at-risk behavior can be attributed to gaps in security policy. Also seen was inadequate enforcement and follow-up to policy violations due to a lack of resources or personnel training. Several subjects were simply able to evade security policies due to IT skills superior to those responsible for enforcement. Education and training to address these gaps should include not only technical vulnerabilities but also security policies, deterrent measures, coworker responsibilities, and consequences for systems and for offending employees resulting from insider abuse. The use of actual case studies such as those included can enhance the effectiveness of these educational efforts.

Lastly, the patterns that emerged from these cases can potentially also aid investigators of insider crime to identify perpetrators. While we may not be able to construct an insider personality profile to facilitate investigation, there are definite patterns in the combined personal backgrounds and work relationships that make these individuals stand out among their peers. The combination of personal characteristics and problematic interactions in the workplace, identified in these case studies as risk indicators, could help narrow a field of suspects or assist investigators and prosecutors to select appropriate case management strategies.

Table of Contents

List of Tables

List of Figures

Introduction

Background

Insider attacks against information technology (IT) infrastructure are among the security breaches most feared by both national and corporate security professionals. In addition to the economic costs of these attacks, insiders' extensive knowledge gives them the capacity to significantly disrupt, destroy, or even seize control of an organization's resources or to contaminate the data contained within these systems. Attacks that cripple any national critical infrastructure have far-reaching domino effects. As such they represent a larger national security issue and, consequently, are a concern of the Department of Defense (DoD).

The 10 cases selected by the Defense Personnel Security Research Center (PERSEREC) for this study have been drawn from the contemporary experience of national infrastructure industries. The U.S. critical infrastructure is defined as including organizations involved in telecommunications, banking and finance, electrical power, gas and oil production, storage or delivery, transportation, water supply systems, emergency services, and government operations. Case selection preference was also given to Defense and government contractors that maintain cleared facilities under the National Industrial Security Program. DoD interest in this study of private-sector events also derives from the fact that its mission is closely integrated with the sensitive and classified work being carried out in its contractor community and that Defense agencies and military facilities are themselves increasingly outsourcing IT functions.

Many of the technically qualified individuals who control and update critical Defense systems are drawn from the same professional pool as were the insider offenders in these case studies. Similarly, where subcontracted personnel are recruited to administer unclassified but critical government systems, little is known about their suitability to hold a position of trust. And typically, as with the employers of the 10 perpetrators described in accounts of this study, nothing is known about their history of information systems misuse.[1]

In addition, while the vulnerability of information systems utilized by critical infrastructure industries is a national defense concern, we have observed that patterns of insider abuse in the private sector are not unlike those documented in Defense agencies and military departments. What can be learned about this form of trust betrayal in one sector has definite relevance for understanding it in the other.

[1] The growing insider problem resulting from the outsourcing of IT professionals is described by Caruso (2003).

Objectives

The U.S. critical IT infrastructure—including our national security networks—is predominantly located on privately owned or operated systems. Acknowledging this fact, we intend to improve our understanding of corporate insiders who violate the legal, organizational, and ethical guidelines covering the security, confidentiality and propriety of these networks and their contents. For the purpose of this study, insiders included individuals with authorized access to an organization's information technology systems, such as employees, contractors, consultants, subscribers or customers, and even authorized competitors.

As with the wider range of research activities that focus on trust betrayal, this effort is based on the assumption that effective policies and programs designed to prevent, detect, manage, and investigate insider offenses must be based on an understanding of the behavior and motivations of the perpetrators involved and especially their interactions in the workplace. In general, the subjects described below used their positions of trust to commit such acts for personal reasons related to their workplace experience. The close parallels between several of the case studies presented here and events that have occurred in the DoD and other federal agencies support the view that trust betrayal regarding IT systems has the same underlying motivations and patterns of behavior regardless of organizational context.[2]

Approach

The full narratives of cases on which this analysis is based are contained in a companion PERSEREC report (Shaw & Fischer, 2005) (FOUO). These cases of insider abuse involved offenders working in one of the critical sectors of the national infrastructure. Each case study discusses the offender's background, the organizational environment in which the offense took place, the details of each event, the offender's presumed motivations, final legal and investigative actions that resulted from the offense or attack, and lessons learned from each incident having implications for corporate policy or national security. Emphasis in these studies was placed on behaviors with implications for policies and procedures related to prevention, detection, management, and investigation of offenses.

In this analytic report, prevention refers to policies and practices affecting the screening and selection of employees and their assignment to tasks. Prevention also includes policies and practices designed to deter these acts. Detection refers to policies or practices that increase the odds that an employee at risk for the commission of such acts will be noticed by personnel in positions to intervene. Management concerns the manner in which at-risk personnel are dealt with in order to reduce the risk of an insider attack or decrease the consequences of an act, should it occur. Investigation refers to efforts to identify, understand and document the activities of an at-risk employee or a perpetrator of

[2] A database of DoD Insider Events being populated at PERSEREC also indicates that approximately 20% of the offenders on DoD systems were contractor employees. Over half of all offenders were system administrators or assistant system administrators.

an insider act. Investigation may be for the purpose of case management and/or prosecution.

This study also offers an opportunity to assess whether the behavior of the subjects and organizations involved in insider betrayal was consistent with previously hypothesized patterns and models of insider activity. The implications of these results for the small but growing literature on insider activity will be examined following our review of findings.

Comparative Case Study Methodology

This study employs the comparative case study methodology that is appropriate for the study of phenomena or behaviors for which we have no established theories, testable hypotheses, or clear understanding of underlying causal factors. Conceptual frameworks for understanding IT insider abuse, however, will be discussed following the review of our findings. Of those frameworks, that which is offered by Gudaitis (1998) is particularly supportive of the case study approach. Gudaitis, a forensic profiler, argues against a single profile of cyber-offenders since the method of developing a single profile (such as that for a serial killer) does not reflect the dynamic nature of individuals or the organizations in which they work.

While the results of case study comparisons as *findings* cannot be generalized with any degree of confidence to a larger universe of cases of the same class or category, what can be gained from this method (that cannot be claimed by larger-sample statistical studies) is an understanding of the contextual factors that surround and influence the event. Sometimes we need to know the whole story—organizational climate, interpersonal conflict, technical systems architecture, personal stress from outside events, mental health of the offender—before we can understand why a given abuse or attack occurred. Not having preconceptions of what we find in each case, we can proceed to recognize and compare common themes present in a limited set of indepth studies. In the present set of cases, for example, disgruntlement appears to be a dominant factor in all but one account. Ineffective management intervention following indications of disgruntlement is another common theme.

We conclude this report by identifying a set of issues or problems that were clearly factors leading to damage, loss, or compromise of critical systems in these all or many of these 10 situations. As is typical of findings from the analysis of comparative case studies, we do not suggest that these situational factors necessarily are present in similar events in other organizations in government or industry. For each finding we have also suggested a possible solution. In an exploratory study of this type, formal policy recommendations may be premature; however, we considered it reasonable for now to state, for example, that since post-termination attacks by disgruntled employees are so frequently seen in this selection of cases, managers and administrators should take a hard look at both termination and remote access policies. In a sense we are setting the stage for systematic inquiries that will more rigorously confirm (or not) the magnitude of risk posed by a given situational factor or a set of interacting factors.

Case Selection

The following criteria were used for case selection:

- The subject's actions should be confirmed by criminal conviction, confession, or other independent, reliable and verifiable means. The insider activities of all subjects, with the exception of the Manipulator (a pseudonym) in Case 10, were confirmed by court findings.
- As noted above, preference was given to cases that involved civilian organizations considered part of the U.S. critical national infrastructure. Priority was also given to Defense and government contractors maintaining cleared facilities under the National Industrial Security Program.
- To minimize research costs and travel expenses, the location of subjects and case materials was limited to the Washington, DC/New York corridor.
- For cases to be included in the analysis, researchers needed access to public or private materials—beyond media coverage—including the possibility of interviewing investigators, prosecutors, subject peers and supervisors, as well as the subject of the investigation. However, the investigator and sponsor both acknowledged the difficulty of obtaining direct subject cooperation in this research. The emphasis on information derived from members of the subject's organization and investigators is consistent with the research objective of developing organizational (as well as individual) indicators of risk and lessons learned that may be used by employees and personnel security specialists to improve their detection, intervention and management of insider risk within the workplace.

Applying these criteria, the investigators developed a list of 15 candidate cases. This list was based on news media reports, specialized information security reports and bulletin boards, and information security and law enforcement contacts. In the first phase of research (2001–2002), the authors selected five of these candidates for indepth investigation. In the second phase (2002–2003), five additional cases were selected for review. During the course of the research it became clear that two of these cases would be tied up in the legal system beyond the planned period of contract performance, limiting access to important case data and the availability of personnel for interview. Two additional cases from the case candidate list were therefore substituted.

To maximize corporate cooperation, in some cases the identity of the corporate subjects and their affiliated organizations had to remain anonymous. However, in such cases an independent individual—subject to the approval of the sponsor—was identified who would know the identity of the interview subjects and cases for data verification. In three of the 10 cases the names of persons and companies were omitted in order to protect their privacy and the relationship between key interview sources and the organization.

Table 1 summarizes the types of data collected across the 10 case studies. The first column gives the number and label for each case. Columns 2–8 refer to the type of data collected. Court Documents refers to materials related to legal procedures in the

case, including indictments, motions, trial transcripts, information related to sentencing, and court decisions. In Cases 1–3 and 5–9 these court documents were related to criminal prosecutions. In Case 4, the court documents were related to civil litigation. There was no legal action in Case 10 as the matter was managed internally, without law enforcement involvement. Case 10 was also notable for its selection source. This case was referred by the employer to the principal investigator, a practicing clinical psychologist, for a private

Table 1
Data Sources by Case

Case Number And Subject	Court Docs.	Investigator Interview	Prosecutor Interview	Law Enforce. Records	Coworker Interviews	Media Records	Subject Inter-view
1. Crasher	X	X	X	X	X	X	
2. Data Destroyer	X	X	X	X	X	X	
3. Hacker	X	X	X	X	X	X	
4. Intruder	X	X	X	NA	NA	NA	X
5. Time Bomber	X	X	X	X	X	X	
6. Extortionist	X	X	X	X	X	X	
7. Saboteur	X	X	X	X	X	X	
8. Thief	X	X	X	X	X	X	X
9. Attacker	X	X	X	X	X	X	
10. Manipulator	NA	X	NA	NA	X	NA	X

X indicates that data were collected; NA that data would be nonapplicable
The subjects of Cases 2, 4 and 10 will remain anonymous due to commitments to their organizations.

consultation. It was used with permission of the organization affected, with the understanding that any published case study would protect the identity of the individuals and company involved. For privacy and confidentiality considerations, we have used a short name, reflecting the type of offense, to identify each case.

Investigator Interview refers to interviews with either private security personnel or law enforcement personnel responsible for investigating the case. In Cases 1, 3, 6, and 8, both types of personnel were involved and interviewed. In Cases 2, 4, and 10, only private security investigators were interviewed. In Cases 5, 7 and 9, only law enforcement officers were interviewed. Prosecutor Interview refers to discussion with the lawyer representing the U.S. Attorney's office responsible for prosecuting the case. Law Enforcement Records refers to reports, interview transcripts, email or other computer records, probation documents and other materials that in a specific case were not part of court documents, but were made available to the investigator by law enforcement agents or others. Coworker Interview refers to discussions with individuals who worked directly with the subject at the organization affected and were directly familiar with him during the period of the event. In Cases 2, 5, 7, 8 and 10, this involved the subject's supervisor as well as other coworkers. In Cases 1, 3, and 9, interviews were conducted with supervisory personnel only. In Case 6, involving a foreign hacker, interviews were conducted with coworkers at the organization targeted. In eight of the 10 cases media coverage of the incident was collected and utilized.

Attempts were made to contact all the insider offenders by phone, email or land mail, except for the Hacker, the Time Bomber, and the Saboteur who were in federal prison. It should also be noted that the Hacker and the Time Bomber publicly denied their guilt, blaming a government conspiracy. The Hacker, the Data Destroyer and the Time Bomber were also being interviewed concurrently by other federal researchers. Federal prison guidelines on human subjects also made the odds of interviews with the subjects during the period of this study extremely unlikely. For example, as of this writing, negotiations are still under way to interview the Extortionist before he is deported.

Possible Selection Bias

The selection of successfully prosecuted cases (with the exception of Case 10) for this study may have resulted in a set of insider events that are not typical in several ways of the larger universe of events.[3] It is generally acknowledged that many insider offenders are not prosecuted due to company concerns about public image. Therefore, prosecuted cases may represent only a minority of insider events. For example, eight of these 10 cases resulted from the actions of insiders who, either under threat of dismissal or following their termination, attacked their employers from remote locations. We cannot say for certain that this characteristic is typical of most or even a majority of insider cases without looking at a much larger and representative sample of events.

In addition, the victimized employers appear to have needed law enforcement assistance to obtain search warrants and to otherwise physically intervene to neutralize the threat. These threats may have been sufficiently significant to offset the potentially damaging impact of publicity. In the one exception to this selection criterion, Case 10, the company still had significant leverage with the subject who was deeply attached to his facility, wanted to hold on to his job and prove his case against his supervisor. This allowed the company to intervene to halt his attacks without the assistance of law enforcement.

As Table 1 reveals, the inability to conduct personal interviews with subjects has been a problem for researchers. Subjects who refused interview requests were anxious to put the event behind them and did not want to generate additional publicity regarding what they had done. Of the three subjects who participated in interviews, the Manipulator (Case 10) was attempting to preserve his job by participating in a company-sanctioned inquiry. The Thief and the Intruder felt they had been unfairly treated and appeared anxious to express this attitude. The remaining subjects did not respond to inquiries. We are left with the possibility that subjects who do participate in interviews may have ulterior agendas affecting the information they provide.

[3] The subject of Case 4, the Anonymous Trader, was not criminally prosecuted, but became the subject of a court order restraining him from the further dissemination or use of the firm's proprietary information.

Data Collection

Data collection followed an Event Case Study Form developed by researchers so that the information obtained would be consistent in scope with information on other insider events maintained in an existing database at PERSEREC. As previously mentioned, the actual case studies contain detailed accounts of the 10 cases or serious insider events that served as the basis for the analysis seen in the following discussion. The following standard outline used in the narrative accounts in Table 2 displays the categories of data that were collected on all cases. The wide scope of coverage of this collection effort facilitated the comparative analysis of specific dimensions of these events, such as motivation or detection, and of interrelated patterns of behaviors and situational contexts. The use of this standard format should assist the reader who wishes to refer back to a particular case for more detailed information as it is cited or discussed in this analytic section (Shaw & Fischer, 2005).

Table 2
Insider Event Case Study Format

Background to the Insider Event
- Subject Background
- The Victimized Organization
- Events Leading to the Offense

Environment in Which the Offense Occurred
- Organizational Context
- Social Climate in the Workplace
- System Characteristics and Architecture

The Insider Event
- Detection of the Abuse
- Type of Offense or Misuse of the System
- Identification of the Perpetrator
- Modus Operandi
- Organizational Response
- Damage to System or Effect on its Operability

Motivations of the Subject
- Assessment by First-Hand Witnesses
- Assessment by Investigative Agents or Prosecutors
- The Subject's View

Investigative and Legal Actions
- Review of Audit Trails and Other Documentation
- Review of Forensic Evidence
- Arrest and Prosecution

Conclusions and Lessons Learned
- Issues Arising from this Case
- Implications for National Security and Impact on the Organization

Findings

This section describes the patterns observed across the 10 cases. Information is discussed in sections covering Subject and Attack Characteristics, Screening, Attack Detection, Organizational and Social Environment, and Personnel Management Issues. This data overview is followed by an assessment and critique of analytic frameworks offered in the growing body of literature on the IT insider offender. In this latter section we address the question of whether, or to what extent, the typologies, hypotheses, and predictive factors proposed by ourselves and other analysts are supported by the data derived from the 10 cases studied in the present research effort.

Subject and Attack Characteristics

Table 3 displays some of the basic personal descriptors of the 10 male subjects identified as the perpetrators of these insider offenses. Half of the subjects worked in the financial and banking industry, two were U.S. government contractors, two others worked in Internet-based telecommunications, and the last subject was from the energy production sector. Their ages ranged from 20–39 years.

Seven were U.S. citizens and the three remaining were Algerian, Brazilian and Russian (the hacker based in Kazakhstan). Half were single and of the five who were married, three had children. Two were employed as system administrators, three were programmers, two were helpdesk staff, one was a chief technology officer, another was a plant automation officer, and another was an investment trader. Their time on the job ranged from 2 months to 15 years. Four were fired or laid off at the time of the attack, three were on probation, and two had resigned and were attempting to negotiate the terms of their severance. The lone foreign hacker—a system administrator at a financial institution—was gainfully employed at the time of his attack. His access to the targeted system was through his company's customer subscription.

The subjects' positions included a broad range of job responsibilities ranging from the most senior to entry-level positions. Eight of nine had physically left the workplace at the time of attack, with the exception of the Extortionist, who attacked from his office in Kazakhstan. The Saboteur and the Thief were both on probation but still at work and managed to attack from their workstations.

Table 4 presents descriptive data on the attacks. As the table indicates, seven of the attacks were directed against organizational databases in attempts to corrupt, copy or destroy the contents. The three other attacks were designed to disrupt and threaten corporate operations and damage the reputation of the business. It is interesting to note that in these three cases the subject was still attempting to place pressure on the organization to advance his employment-related goals (severance, consulting or job retention). The damage resulting from these attacks ranged from labor for repairs and loss of reputation to over $10 million. As noted above, all but two of the attacks came from remote locations, with the subject using his system knowledge to gain unauthorized access.

Table 3
Subject Characteristics for 10 Cases

Subject and Victimized Organization	Subject Data	Position	Time On Job	Job Status At Time of Attack	Industry/ Sector
1. The Crasher	34 years, Algerian male, single	Programmer, Analyst	2 mos.	Quit, Negotiating	Wholesale Brokerage
2. The Data Destroyer	34 years, male, Asian/American, single	Programmer, Analyst	34 mos.	Fired	International Insurance
3. The Hacker	29 years, Hispanic male, U.S. citizen, married	Programmer, Security	4 mos.	Laid off	Venture Capital
4. The Intruder	34 years, White male, U.S citizen, single	Investment Trader	18 mos.	Fired	Int'l. Bank Investments
5. The Time Bomber	36 years White male, U.S. citizen, married with 4 children	System Administrator	11 yrs.	Fired	Defense Contractor
6. The Extortionist	30 years, Russian male, married with 1 child	System Administrator, Programmer	20 mos.	IT Manager	Investment
7. The Saboteur	20 years, White male, U.S. citizen, single	Webmaster, Part-time System Administrator	2 mos.	Probation	Government Agency & Contractor
8. The Thief	23 years, White male, single, Brazilian	Network helpdesk	19 mos.	Probation	Internet Service Provider
9. The Attacker	39 years White male, U.S. citizen married with 1 child	Chief Technical Officer	22 mos.	Resigned	Web Applications Software
10. The Manipulator	37 years, White male, U.S. citizen married	Plant Automation Officer	15 yrs.	Probation	Petroleum Industry

There has been considerable debate over whether the consequences and sentencing for computer crimes are sufficient to warrant bringing charges, or significant enough to deter attacks (MSNBC, 2000). The final column of Table 4 contains information on the legal consequences for the subject. With the exception of Cases 4 and 10 which were not criminally prosecuted, the consequences for the offender ranged from 3 months' probation to 51 months in prison. For the six subjects sentenced, the mean prison time was 27 months, with a range from 10 to 51 months. It is interesting to note that the lightest prison sentence was given in 2000 to the Crasher in Case 1, while the heaviest sentence of 51 months was given in 2003 to the Extortionist. While the attacks and their consequences are not uniformly compatible, prison sentences appear to be getting more severe over time.

Table 4
Attack Data by Case

Subject and Victimized Organization	System Affected	Type of Attack or Offense	Damage	Attack Site	Consequences For Subject
1. The Crasher	Client server	DOS attack using inside knowledge	Service loss, >$100K	remote	10 months prison, 2 yrs. supervised release, $20K restitution
2. The Data Destroyer	HR database	Unauthorized access, destruction, corruption of data	Service loss, $91K	remote	18 months prison, $91K restitution
3. The Hacker	Point of sale databases	Unauthorized access, destruction of databases	Service loss, >$100K	remote	27 months prison, $96K restitution
4. The Intruder	Client trading databases	Theft of proprietary data	Service loss, $500K	remote	Civil injunction
5. The Time Bomber	Manufacturing databases	Use of time bomb	Service loss, layoffs, >$10 million	inside	41 months prison, $2 million restitution
6. The Extortionist	Private financial information system	Used access as customer to hack system, extortion	None to system, confidentiality, reputation	remote	51 months prison, will be deported
7. The Saboteur	Inventory control databases	Unauthorized access, time bomb	System loss	inside	15 months prison, 3 yrs. supervised release, $108K restitution
8. The Thief	ISP engineering databases	Leaked data to unauthorized competitor	None to system, loss of proprietary data, competitive advantage, reputation	inside	6 months probation
9. The Attacker	Email, voicemail	Unauthorized access w/backdoor	Loss of service, reputation	remote	3 months probation, $5K fine
10. The Manipulator	Plant safety and control systems	Withheld password, sabotage	Loss of access to safety controls, threat to plant safety	remote	Terminated employment

Screening

Table 5 examines screening issues for each employee. As the second column indicates, no basic background checks were completed on any subject at the time he was hired. A formal background check on the Saboteur was returned shortly after his attack, with a recommendation against hiring. Family connections played a role in hiring in three cases. Five of the subjects had a history of significant risk factors at the time of their hiring that went undetected. The insurance company programmer in Case 2 had prior convictions for fraud and a history of harassment requiring a restraining order. His attacks at his new employer included sexual harassment and the corruption of the company database. The Hacker from Case 3 had a prior conviction for drug trafficking and was a widely published hacker with his own Web site including hacker propaganda and technical tips. The Saboteur from Case 7 also had a history of drug problems and convictions. The Attacker from the Internet provider in Case 9 informed his employer of a previous conviction as a youth for destroying property during an act of anger.

Based on these results, the addition of formal screening efforts, such as a criminal records check, would have improved hiring decision-making in three of the 10 cases. The informal practice of Internet searches by name or pseudonym (if available) could have added important information to hiring decision-making in three of the 10 cases involving subjects who were well-known hackers.

Column 4 describes the presence of tracking problems defined in two ways. First, if the employer involved in this case was unaware of the subject's previous illegal or at-risk activities, a tracking problem was noted. Second, if after leaving the employer under study the subject was hired by another organization, which was also unaware of the violation under study, a tracking problem was noted. For example, the insurance company employee from Case 2 attacked his former employer from his new employer's site. His new employer was unaware of his activities at the insurance company. Even when his new employers were made aware of these attacks, they initially refused to grant assistance to help end the intrusions.

The Hacker, from Case 3, was fired from his previous position for attempting to extort security fees from Web sites after attacking them to expose their vulnerabilities. His attack of concern in this investigation involved using his former employer's access to the target in order to convince a potential client of the need for his group's security services. The Saboteur from Case 7 had attempted to save his job and extort employment terms from his previous employer before working as a contractor at the IRS. At the time of this research, he was employed again as a programmer until his employer learned of his activities at the contractor under study. A review of the Saboteur's criminal record since the incident showed several arrests related to drug sales, evading arrest, and accessory to murder.

Table 5
Personnel Screening Issues by Case

Subject and Victimized Organization	Screening/selection Problem	Prior known offenses or undetected risk factors	Tracking Problem
1. The Crasher	Referred by brother, professor, no background check	No	No
2. The Data Destroyer	No background check	Multiple prior offenses: forgery, grand larceny, disorderly conduct	Yes
3. The Hacker	No background check	Prior conviction, published hacker	Yes
4. The Intruder	No background check	No	No
5. The Time Bomber	No background check	No	No
6. The Extortionist	N/A (overseas client)	No	No
7. The Saboteur	Delayed background check	Prior hacking, extortion	Yes
8. The Thief	No background check, recommended by brother	Published hacker	No
9. The Attacker	No background check	Yes (juvenile)	No
10. The Manipulator	Hired by father, no background check	No	No

Attack Detection

Table 6 describes detection issues across the 10 cases. The subjects in these cases committed several different types of attacks, including the placement of time bombs and attacks designed to have immediate effects. One measure of the effectiveness of computer and personnel security is the speed with which organizations react to these threats. It was especially important to determine whether prompt investigation of a threat or risk factors led to defusing or preventing damage from these threats. The second column in Table 6 shows whether the affected organization discovered the attack immediately or whether its detection of the problem was delayed. Data on the detection of attack preparation and its rehearsal or planning, if they existed, were not captured and are not evaluated here—we dealt solely with the discovery of the attack under study.

As the table indicates, in all but three cases the attack was discovered as soon as the system was accessed by legitimate users. This result has more to do with the nature of the attacks employed and the personnel context surrounding the attacks than the detection ability of the companies involved. For example, the attack by the anonymous programmer in Case 2 targeted a payroll database. It was not discovered until a routine company audit 3 months after the subject's termination. On the other hand, the Saboteur, in Case 7, made explicit threats toward his supervisor that led to a review of his recent activities. It was this review, several hours after the threat, that led to the discovery and defusing of his time bomb. The Thief in Case 8 transferred engineering plans to a friend

from a competitor, that were subsequently posted on the Web. His company did not discover the theft until it was reported by an acquaintance of the subject, weeks after the theft. The other attacks were such that the results had an immediate impact on system operations.

Table 6
Detection Issues by Case

Subject and Victimized Organization	Detection Delayed	Subject OPSEC	Total Time Employed	Advance Knowledge of Disgruntlement	Company Intervention
1. The Crasher	No	Yes	2 months	2 months	2 weeks
2. The Data Destroyer	Yes	Yes	34 months	16 months	16 months
3. The Hacker	No	Yes	4 months	1 month	None visible, Deception
4. The Intruder	No	No	18 months	7 months	12 days
5. The Time Bomber	No	Yes	11 years	4 years	14 months
6. The Extortionist	No	Yes	NA	NA	NA
7. The Saboteur	Yes	Yes	2 months	1 month	1 month
8. The Thief	Yes	Yes	19 months	6 months	6 months
9. The Attacker	No	Yes	22 months	2 months	2 months
10. The Manipulator	No	Yes	15 years	19 months	19 months

The third column in Table 6 describes whether the subject employed an operations security (OPSEC) strategy[4] to hide his attack planning, the attack itself, or clues to his identity associated with the attack**.** Nine of the 10 attackers took such steps, ranging from elaborate efforts to mask their remote access address (Cases 1–3, 6, and 9) to the use of time bombs (Cases 5, 7), and the use of collaborating partners who were still inside the organization (Case 10). The Time Bomber in Case 5 appears to have engaged in active attack planning and rehearsal while using his administrative powers to centralize computer operations and eliminate back-ups not under his control in preparation for his attack. The trader in Case 4, who did not engage in covert methods, appears to have reacted impulsively and did not intend to cause the damage associated with his theft of proprietary data.

Columns 5 and 6 display data on the visibility of personnel problems prior to the attack. Column 5 indicates how much in advance of an attack the company was aware of the subject's disgruntlement, while Column 6 displays data on whether management intervened and if so, how long before the attack. As the data in Column 5 indicate, signs of disgruntlement in the nine subjects (where disgruntlement was relevant) appeared from 1 to 48 months before the attack. The time period prior to the attack, during which there were active problems requiring company intervention, ranged from 12 days to 19 months.

[4] An OPSEC strategy would be one in which the offender engaged in a systematic attempt to prevent the display or visibility of any indicators of unauthorized or illegal activities under way.

These results are extremely important for the detection of insider risk because they indicate the existence of a window of opportunity during which effective employer intervention can reduce the risk of an attack. In addition, the findings indicate that in three of the cases this window could have been expanded by weeks and months, if the subject's disgruntlement had been discovered sooner. As discussed below in Tables 8 and 9, the results show that management interventions for these subjects did not avert the attacks, and in some cases, contributed to increased attack risk.

It should be noted that the offender in Case 3, who gave no forewarning of his attack, appeared disgruntled about his layoff, without full payment of back wages owed, by a company owned by the venture capital (VC) firm with which he was dealing. This firm was considering backing his venture company into computer security when he attacked one of their other companies using access he had gained while working in their offices. This anonymous attack was designed, the offender claimed, to demonstrate the company's need for security services. It appears that he was hiding his anger about his layoff in order to encourage the VC firm to back his new enterprise.

Table 6 also summarizes the emergence of subject disgruntlement compared to time on the job at the time of the attack. For example, the Crasher became disgruntled almost immediately on entry into his firm because he became embroiled in an ongoing conflict to which he was connected by his brother and former professor. In contrast, the Manipulator's difficulties with his supervisor did not begin until he had been on the job for over 13 years. Of his 180 months of tenure, he spent less than 10% actively disgruntled (above his normal level of anger) and his disgruntlement did not emerge until he had completed 90% of his tenure. As Table 6 indicates, disgruntlement occurs across a range of times in the job cycle, but was more common in the third (44% of subjects) and fourth (33% of subjects) quarters. Based on what we see in this limited set of cases, disgruntled subjects do not necessarily "select themselves out" early in the job cycle. Not surprisingly, the odds of disgruntlement appear to increase with time on the job.

While this study focused on human factors rather than computer safeguards, there are implications here for security technology. While specific security technologies in each case might have aided earlier detection, these results indicate that the more important overall risk factors were the screening issues that were missed and the personnel problems that arose prior to the attacks accompanying subject disgruntlement. In addition, as column three on Table 6 indicates, nine out of the 10 subjects utilized some type operations security to overcome safeguards and to protect their identity. The sophistication of these subjects and their efforts at deception indicate the likelihood that they would have been aware of, and have taken steps to neutralize, additional computer security measures.

Finally, eight of the 10 organizations involved did become aware of the employee risk, but their interventions were unsuccessful. Specific examination on a case-by-case basis could likely result in the post-hoc design of security software which could have warned of the increased risk or of violations in these cases. For example, the Saboteur's earlier violations were detected by such safeguards and he was sanctioned for his

behavior. However, this did little to prevent his subsequent attack. Analysis of potential security tools is beyond the scope of our expertise. In addition, the data indicate that there are opportunities for significant improvements in insider abuse prediction and detection and systems management by addressing behavioral factors. But it is our hope that technical experts will use these cases to examine and perhaps update computer security applications.

Organizational and Social Environment

Table 7 examines the 10 cases in terms of the presence of organizational and personnel stressors, social and/or cultural conflicts in the workplace, overdependence on the subject by management, and the presence or absence of personnel and security policies and enforcement relevant to the attack.

Table 7
Organizational/Management Issues by Case

Subject and Victimized Organization	Organiz. Change/ Personnel Stressors	Social/ Cultural Conflicts	Over-Dependence On Subject	Policies Lacking	Policy Implementation Problems
1. The Crasher	Yes	Yes	Yes	Yes	No
2. The Data Destroyer	Yes	Yes	Yes	Yes	Yes
3. The Hacker	Yes	No	Yes	Yes	No
4. The Intruder	Yes	No	Yes	No	Yes
5. The Time Bomber	Yes	No	Yes	Yes	Yes
6. The Extortionist	Yes	NR	NR	NR	Yes
7. The Saboteur	Yes	Yes	Yes	Yes	Yes
8. The Thief	Yes	Yes	No	Yes	Yes
9. The Attacker	Yes	Yes	Yes	Yes	Yes
10. The Manipulator	Yes	Yes	Yes	Yes	Yes

* NR=not relevant

Organizational Change and Personal Stress

Organizational issues are defined as affecting the whole enterprise or facility involved and may be as broad as layoffs, mergers, extreme financial distress, or other organizationwide pressures. Personnel issues are defined as personal work-related issues affecting the subject directly, such as a demotion, change in supervisor, a personal conflict, or work-related disappointment. For example, in Case 9, on an organizational level, layoffs were spreading after 9/11 and when the Internet bubble broke, reducing demand for his company's services. At the same time, on a personal level, the Attacker had reportedly had a problematic relationship with a subordinate and was also facing financial distress. In Case 10, on an organizational level, the petroleum processing plant had lost money so consistently that it was in danger of closing and company officers were

desperate for a means to improve productivity. On a personal level, the Manipulator deeply resented the appointment of a nontechnical, process-oriented supervisor who sought to curtail his autonomy and influence over plant operations. As Table 7 indicates, there were organizational and/or personnel stressors present in the work site in all 10 cases. Social and/or cultural conflicts in the workplace played a role in six of the nine cases considered. Overdependence on the subject was an issue in eight of the nine cases. Table 8 below contains a list of personal stressors for each of the subjects.

Table 8
Examples of Personal Stressors by Subject

Subject	Personal Stressor
1. The Crasher	Loss of mentor at work, feeling exploited, replaced by new technical team
2. The Data Destroyer	Rejection by love object, feeling betrayed by her, loss of job, embarrassment of being caught on video violating rules and lying
3. The Hacker	Loss of job without warning, loss of pay for periods of work, loss of access to computer resources
4. The Intruder	Feeling betrayed, criticized, demoted, fired by coworkers he thought were friends
5. The Time Bomber	Demotion, interpersonal conflict with coworkers, death of mother w/in year due to asbestosis, diagnosed with epilepsy w/in year, exacerbation of other medical problems
6. The Extortionist	Professional and financial frustrations—feeling stuck in Kazakhstan
7. The Saboteur	Interpersonal conflicts, security and HR warnings, demotion, criminal and drug activities
8. The Thief	Parents' separation, brother's departure, frustrated in efforts to get training, advancement, recognition, placed on probation
9. The Attacker	Financial stress, marital problems, conflicts with superiors
10. The Manipulator	Wife's terminal illness, loss of job autonomy, rejection by coworker, loss of overtime pay, alcoholism, conflict with supervisor, coworkers

Social and Cultural Conflicts

Social and cultural conflicts refer to differences between social, racial, or technical groups leading to tensions and conflict between the subject and others. For example, in Case 1, the predominantly academic and Middle Eastern software development staff at the subject's firm were being systematically laid off as the firm introduced software engineers with production experience who were not Middle Eastern. In Case 7, the Saboteur was accused of making racial comments toward his African-American supervisor and was self-taught in computers while the majority of other staff were academically trained. In his attacks on his former employers, the Attacker, in Case 9, also described the financial background and social status of other employees as a source of his resentment.

Overdependence on the Subject by Management

Overdependence refers to the level of the organization's reliance on the subject. An over-dependent condition was deemed to exist if the subject had managerial control over the enterprise, out of proportion to his technical position, due to specialized system knowledge, access, or control. In cases of overdependence, the level of influence exceeded the guidelines of standard security practices controlling an individual's ability to inflict harm, such as "two-person" accounting rules, the need for monitoring, back-ups, redundancy, etc. As the president of the firm noted in the Attacker's case, "the servant had become the master." For example, in Cases 1, 5, 9 and 10, the enterprises found themselves at the mercy of former employees who were able to shut down critical systems in a manner that endangered the well-being and survival of the company. The subjects in these instances were able to achieve this level of control due to the unique access and knowledge they had acquired.

For example, in Case 5, the Time Bomber had such control over production IT policies and practices that he was able to eliminate all back-ups, except those centrally controlled by him, and plan and rehearse his attack without detection. Senior management's long reliance on the Time Bomber also appeared to make him invulnerable to firing, even after his having committed serious personnel violations. In this regard, there are many striking parallels between the Time Bomber case and the recent case of FBI employee Robert Hanssen. Both employees were cited for personnel violations prior to their attacks. Both were accused of physical violence toward female employees and both were shielded from supervisors who wanted their employment terminated. (The reader is referred to Report 2 for an in-depth review of the Time Bomber case.) In Case 9, the Attacker was the only employee who knew how to access programming and safeguards for the company's Web site and voice mail. In Case 10, the Manipulator was the only employee who had the password to the plant's safety controls that were, according to an outside audit, idiosyncratic.

Lack of Policy or Policy Implementation

Column 5 in Table 7 indicates that policies covering the issue leading to disgruntlement, or which could have deterred or prevented the attack, were lacking in eight of nine cases. Policy implementation was a problem in eight of the 10 cases. Case 6 was included in this analysis because the subject's firm had not kept current in its payments for the use of the firm's financial system, and system access should have been terminated long before the attack, based on the provider's policies. However, it is not clear whether a timely termination of access would have deterred, delayed, or prevented the attack. Table 9 below breaks down the absent or non-enforced policies by examples for each case.

Personnel Management Issues

As Table 6 above indicated, there were significant delays in management interventions with these subjects. We also looked at two other important issues that relate to the effectiveness of personnel management efforts. First, how effective were management interventions when they occurred? Second, when a management intervention involved termination of an employee, how did it impact the likelihood of an attack? Other personnel management issues examined in this section include a review of the elapsed time from termination/probation until the attack and the type of management interventions attempted in these cases.

Effectiveness

In two of the 10 cases, management failures facilitated the attack. In Case 6, the offender, the Extortionist, attacked a system from another organization overseas. While his firm had no opportunity to intervene as in the case of a disgruntled employee, the Extortionist's access to this system should have been terminated when his company failed to pay for its subscription. It was not. In Case 3, management had no knowledge of the offender's disgruntlement or identity until he was arrested and charged with a federal crime. However, management facilitated the attack by entertaining the Hacker's overtures for financial backing for a computer security firm and marketing his efforts to another company.

In eight of the 10 cases management intervened but their efforts were ineffective. For example, the Saboteur in Case 7 was highly valued for his technical competence, but according to his supervisor's report, management moved too slowly to intervene in response to the offender's adverse behavior and security violations As noted above, the Time Bomber in Case 5 had been counseled repeatedly regarding his treatment and physical intimidation of fellow employees. Eventually he was demoted and recommended for termination. He was also receiving medical treatment for neurological and psychiatric disorders. The organization did not integrate knowledge of these medical problems into a coherent plan to deal with the Time Bomber's difficulty on the job.

Termination Problems

Because eight of the 10 cases involve attacks after an employee's termination or departure from the work place, it is important to focus on how well the company handled the termination process. The data clearly indicate that the departure of the employee from the job site did not reduce the risk of attack and that in each of these situations termination was poorly handled. For example, in Case 1, the Crasher and his brother resisted efforts to turn vital code over to a new software team. They stopped cooperating and demanded an improved employment contract. The brothers then entered into negotiations with management over conditions for their departure while the CEO was on vacation. Their failure to understand the firm's intellectual property rights, miscommunications during the negotiations, and changes in management's negotiation team, along with other factors, appear to have contributed to the failure of negotiations.

Table 9
Absent or Unenforced Policies or Practices Related to the Event

Subject	Absent Policy or Practice Contributing To Disgruntlement or Which Could Have Prevented Attack	Policy or Practice In Existence But Not Implemented/Enforced
1. The Crasher	Clarity over ownership of intellectual property	
2. The Data Destroyer	Prohibition on Informal Helpdesk activity, privacy safeguards governing IT staff	Reporting of sexual and computer harassment
3. The Intruder		Safeguards against remote access after termination
4. The Hacker	Basic password protection rules, basic system monitoring for dangerous hacker programs, disarming of safeguards	
5. The Time Bomber	No policy preventing IT dependence on individual already on probation, no monitoring of system for dangerous computer activities such as attack rehearsals	Earlier termination for cause thwarted by bureaucratic politics, no enforcement of ban on taking computer equipment home, no EAP referral or medical evaluation for mental health issues after personnel problems arose
6. The Extortionist	Lack of technical safeguard against his hack	Failure to terminate access after non-payment of fees
7. The Saboteur	Lack of system monitoring for hacker tools, activities	Lack of follow-up on personnel and IT violations prior to attack
8. The Thief	No limitations on computer or physical access for persons on probation, no prohibition on sending sensitive data out of network over web or to courtesy computer in lobby	Policy on restricted weekend access by outsiders violated
9. The Attacker	One individual with sole access to and knowledge of critical systems, one individual with sole password access to critical system, clear understandings of pay reductions related to poor business performance	Standard HR policies on inappropriate interpersonal behaviors violated without consequences
10. The Manipulator	One individual with sole access to and knowledge of critical systems, one individual with sole password access to critical system, policies on inappropriate interpersonal behaviors and consequences	Personnel rules governing inappropriate interpersonal behavior were not enforced due to subject's political connections

In Case 3, the Hacker was laid off without prior warning while still owed back pay. In Case 7, the Saboteur was able to access his supervisor's personal files and read his draft termination letter prior to a full decision regarding his employment. In most of the cases described, security measures designed to block the subject's access after termination were lacking.

Time from Termination/Probation Until the Attack

Figure 1 displays the elapsed time for nine of the subjects from the date of termination (or probation for the two employees not terminated—the Thief and the Manipulator) to the date of attack. The elapsed time ranged from 4–5 hours to 85 days.

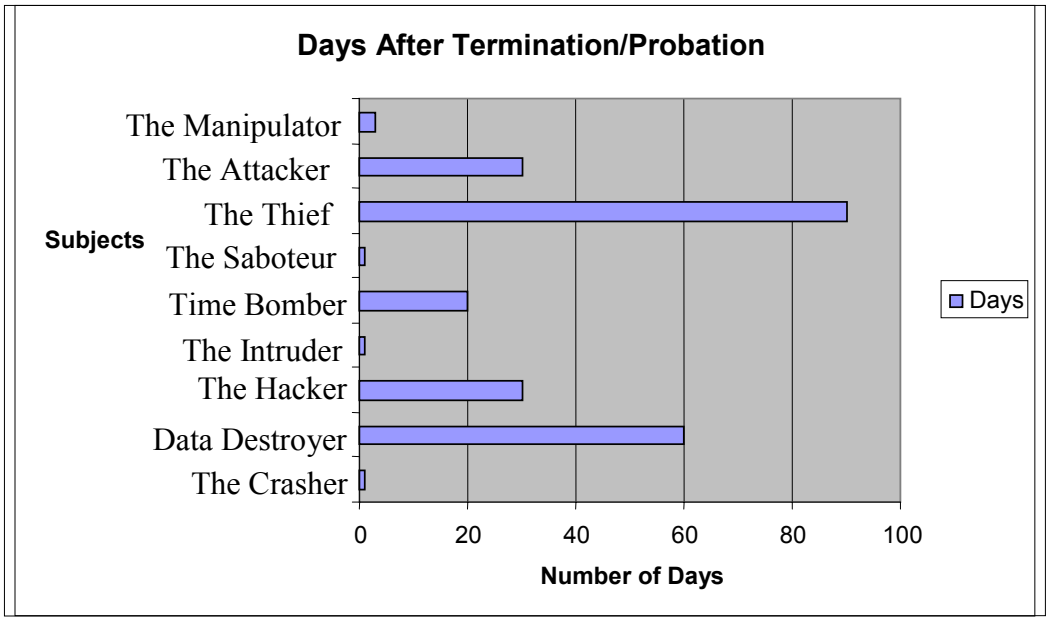

Figure 1 Time from Termination or Probation to Attack.

The cases fall into two distinct groups reflective of the impulsiveness or planning involved in the attacks. The Manipulator, the Saboteur, the Intruder and the Crasher all reported acting impulsively to job-related setbacks. The Attacker, the Thief, the Time Bomber, the Hacker, and the Data Destroyer all acted with deliberation and planning. The Attacker, the Data Destroyer, and the Hacker were also involved in ongoing struggles and relationships with persons from their former companies after their departure. Developments in these ongoing relationships appear to have contributed to the timing of these attacks. For example, even after leaving the workplace, the attacker continued to fight for the compensation he thought he was owed and needed, to improve his financial situation. The Hacker was in negotiations for a new position with the investors of his former company and the Data Destroyer continued after his departure to stalk his love interest at work. The timing of the Thief's attack appears to have been related to his relationship with his accomplice and hacker colleagues, who encouraged him and helped plan the theft. This finding regarding delayed attacks indicates the potential contribution of unresolved employment issues, continued involvement with a former employee, and a subject's unresolved feelings regarding the employer to long-term attack risk.

The findings also indicate that, similar to some violent crimes (Ressler et al., 1980), it may be possible to profile attack risk, type and timing depending on a subject's personal characteristics and the type of employment problems leading to sanctions. For

example, the Manipulator, the Attacker, the Saboteur, and the Crasher were described by peers as being impulsive (the Saboteur and the Manipulator also had substance abuse issues) and their attacks fit this description. Although the Attacker's major action occurred over 30 days after his departure, less destructive, impulsive unprosecuted attacks were reported prior to this time.

Attempted Interventions

Table 10 describes for nine of the subjects the types of interventions employed by management prior to the attacks. As the table indicates, there was a range of efforts to intervene with these employees prior to their termination, ranging from counseling, to negotiations, to suspension. Taken together, the results from Tables 6 and 10 raise a number of interesting questions regarding management interventions in these cases. As Table 6 established, earlier employer awareness of subject disgruntlement may provide a larger window period for intervention. However, in order for these interventions to be effective, they must, if possible, address the underlying issue that places the employee at risk within the work context. For example, the Thief's supervisor was aware of his

Table 10
Management Interventions Prior to Attacks

Subject and Victimized Organization	Management Intervention Prior to Attack
1. The Crasher	Negotiations over pay, options, job, security, then termination of negotiations
2. The Data Destroyer	Investigation without intervention followed by confrontation of evidence and dismissal
3. The Hacker	Abrupt lay-off followed by efforts to help finance start-up security firm
4. The Intruder	Probation
5. The Time Bomber	Counseled, transferred, demoted
7. The Saboteur	Probation under threat of dismissal
8. The Thief	Probation for lateness, Web surfing
9. The Attacker	Counseled, no consequences
10. The Manipulator	Suspension

general disgruntlement but not the cause, in large part due to his lack of communication regarding his complaints (except to his hacker peers). The symptoms of his disgruntlement were, therefore, addressed with discipline (placed on probation for tardiness and Web surfing) alone, while his unhappiness at not being promoted or transferred to engineering and his upset with company advertising never surfaced. According to the Thief, this intervention only increased his frustration with his employer.

Management actions in the cases of the Attacker, the Time Bomber, the Saboteur, and the Manipulator were also reported to have made conditions worse and increased the

risk of attack. This finding indicates that more thorough investigation of underlying personnel issues prior to management interventions may increase the effectiveness of these efforts. The case of the Manipulator illustrates this point. After his initial attacks he was placed on suspension and a management team, including a mental health/security specialist, was formed to deal with the threat he posed to his facility. A long-term management plan, including medical and behavioral assessments and interventions and monitoring, eliminated further incidents, during a difficult period that included the death of his wife and his termination from the organization.

While the results indicate that management interventions with disgruntled employees may be improved, they also highlight the possibility that there may be little that management may do in some cases to prevent these attacks. This finding places greater importance on the need to improve termination procedures, as well as the importance of more serious attention to defensive security measures against former employee who have had system access over a long-term time period.

Relevance to the DoD Insider Threat

While case studies selected for analysis in this report were limited to private sector events involving national infrastructure industries, these insider events are very similar to those that have occurred in DoD agencies and components. In the latter group, based on data on over 80 insider events, 20% were attributed to attacks or misuse by systems administrators while another 75% were committed by insiders with limited administrative access beyond that of a normal or end user. About 60% of the events were the result of malicious or criminal intent and about the same proportion resulted in serious damage or compromise to a system.

What is different about the private sector cases is that in this selection (that we do not claim to be representative of the universe of private sector cases) all but one abuse resulted wholly or in part from a disgruntled employee's attempt to seek revenge or recognition. Among DoD cases in our database, the frequency of disgruntlement is much lower. Many of the DoD offenders misused a government system for personal convenience or advantage without intent to harm. There is no reason to doubt that widespread nonmalicious misuse of systems also takes place in the private sector. These types of events have simply been outside of the scope of the present study. Otherwise, little seems to distinguish insider offenders in DoD organizations from the 10 described here in terms of motivation or method of attack. On a case-by-case basis, we see close parallels between specific DoD and other government agency events and several of the 10 critical infrastructure cases (Fischer, 2003).

U.S. Army: Multiple Attacks

Among the many events that could illustrate this point is that of a Private First Class (PFC) who had helped to develop the U.S. Army's database for enlisted records. This junior service member was responsible for three events, each separated by several

months.[5] The private's history of offenses is similar that of the Saboteur (Case 7) whose repeated abuse of access privileges resulted in conviction and imprisonment.

When first arriving at his duty station in 1995, the PFC reported to an officer who depended upon his computer skills and gave him considerable freedom on the job. The PFC's work position was information systems operator and software analyst, and he was assigned to the Information Support Agency Enlisted Records and Evaluation Center (EREC). A subsequent branch chief, however, was determined to exercise greater authority over his staff and in fact ordered the private to remove unauthorized personal files from the system server. The soldier's resistance to this policy resulted in a nonjudicial punishment in November 1998.

After continued animosity between the private and his new branch chief, the PFC apparently attempted to get even by disabling the system users' accounts in April 1999, resulting in a shutdown of the EREC database system for about 3.5 hours. The PFC was accused of damaging computer information and of unauthorized computer access. Action against the service member resulted in another nonjudicial punishment by which he was reduced in rank, fined, and removed from all systems administrator-level work-related duties.

But the offender was still intent upon revenge. With the assistance of a chat room acquaintance located in Jamaica, he was able to steal passwords and infect several of the workstations on his organization's system with a Trojan virus (BO2K) which gave him remote control of these workstations. He then proceeded to delete over 1,000 work-related files of systems users. The culprit was not difficult to identify by special investigators. In September 1999, the soldier was arrested and his residence searched for evidence. Later that month, an unlawful intrusion was detected by a U.S. Army computer network and traced to someone attacking from Montego Bay, Jamaica.

For this final attack on the Army system, the private was formally prosecuted and was sentenced to a reduction to the lowest enlisted rank, loss of all benefits and pensions, and 4 months of criminal confinement to be followed by a Bad Conduct Discharge.

U.S. Coast Guard: A Remote Attack

Another prosecuted case involved a disgruntled government civilian employee of the U.S. Coast Guard that has a close resemblance to the behavior of the Time Bomber (Case 5) who rigged a time bomb that destroyed his company's production files after his departure from the organization. In early 1998, a civilian employee and systems administrator for the U.S. Coast Guard in Washington, DC, from her home used the password and identification of another employee to gain access to the Coast Guard system after she had resigned from the organization. She was reportedly angry over the fact that the organization had ignored her reports about improper conduct by an IT

[5] Information on this case summary is based on interviews with personnel at the scene of the offence, interviews with case agents, and transcripts from the court martial proceedings.

contractor employee. She had in fact filed a complaint with the Equal Employment Opportunity Commission claiming that she was subject to a hostile work environment.

Two months later, other employees noticed that critical files had been deleted from the Coast Guard nationwide personnel database, causing the system to shut down. According to a news report, "The July crash wiped out almost two weeks' worth of personnel data used to determine promotions, transfers, assignments and disability claim reviews for Coast Guard personnel nationwide" ("Woman gets five months," 1998). The prosecuting Assistant U.S. Attorney stated, "It took 115 Coast Guard employees across the country working more than 1,800 hours to recover and reenter the data, at a cost of more than $40,000."

It was clear that, because of the precision by which the hacking was accomplished, the culprit was an insider or had inside information. The former employee was linked to the crime by the FBI through computer and phone records and the fact that she had used an access code, known only to a few people, to enter the system. She had helped to build the personnel database she later attacked. While claiming that she had not intended the computer system to crash, she did plead guilty to unauthorized access and deletion of files. The offender was sentenced to 5 months in prison, ordered to pay $35,000 of restitution to the Coast Guard, and placed on several months of home detention. She later stated to a media reporter, "I wanted to get even with them. I was frustrated and depressed because no one listened to my complaints of sexual harassment in the workplace. I did delete information, but I did not crash the system" (Coast Guard, 1998). She was also similar to the Time Bomber in her chronic interpersonal problems on the job and her history of psychological issues related to her workplace behavior.

U.S. Air Force Academy: Destructive Hacking

In the final example, a cadet at the U.S. Air Force Academy was accused not only of misusing the academy system for personal chat room activity, but using it as a platform from which to launch a criminal attack on companies in the private sector (Academy Jurors, 1999). A close parallel exists between this insider event and that of the Hacker (in Case 3) who, from his own firm, hacked into the system of another company to destroy sale and inventory files causing over $100,000 damage.

A second-year cadet, along with other cadets, was ordered to stop using Internet chat rooms out of security concerns. Several months later he resumed active participation in chat rooms with the assistance of several cyber-friends not connected to the Air Force. He in fact set up an Internet relay chat room (IRC) server on his PC that was connected to the USAF Network. Unfortunately, his "friends" were engaged in extensive hacking around the Internet and involved the cadet in their activities. At the time the cadet claimed that he had no idea of what these people were doing. In November 1997, the Air Force Office of Special Investigations searched his room and seized his computer. The cadet was initially charged with using the Air Force system to illegally enter three companies and cause $80,000 damage. Two of these charges were later dropped.

Prosecutors argued that he used the Air Force platform to connect to the Internet, and then hacked into company systems, erased data, and planted destructive programs.

In March 1999, the cadet was found guilty by court martial for using an Air Force system to break into and damage a private company's computer system, causing $6,000 damage. He was dismissed from the academy and the service (Air Force Academy, 1999).

Findings from DoD Cases

The following conclusions, published earlier (Fischer, 2003), are based on the analysis of information from the PERSEREC insider database and DoD case studies that have provided insights into the patterns of activity associated with attacks on sensitive information technology resources. These eight observations have been reinforced by what we also see in the 10 cases of insider abuse directed at national critical infrastructure systems. The cases that are particularly illustrative and supportive of each observation from the DoD cases are shown in brackets.

- Technical security measures offer minimal protection from abuse when the offender is a systems administration or has some level of administrative access to the system. [Cases 1, 3, 5, 7, 9,10]
- Interpersonal relations within the workplace and the organization's climate are very important for understanding IT systems misuse. In almost a quarter of the cases there was evidence of prior hostility in the workplace involving the offender and usually a supervisor. [Cases 1, 5, 7, 9, 10]
- Some of these events could have been avoided by better security education. Personnel need to know what the rules are concerning the use of the system, what is an acceptable and not an acceptable use of that system, and what the consequences are for stepping over the line. [Cases 2, 3, 7]
- Both enhanced personnel security and technical deterrents should be applied to minimize the threat posed by angry or indifferent personnel who have legitimate access to defense information systems. [Cases 1, 2, 4, 5, 7, 9, 10]
- Many offenses occurred after discharge or transfer to a new duty station—within 60 days after separation—indicating the need for greater attention to discharge security and personnel planning. [Cases 2, 4, 9]
- Several attacks involved employee remote access to the corporate system, indicating a need for a review of safeguards covering this practice. [Cases 2, 6, 9]
- In several cases examined, a lack of personnel and/or security policies can be cited as having contributed to the event. [Cases 1, 2, 10]
- In some cases, evidence of disgruntlement or performance problems was visible to management well in advance of an attack. Delay in intervening in the underlying personnel problem contributed to the episode or failed to divert the subject from his destructive path. [Cases 7, 9, 10]

Assessment and Critique of Analytic Frameworks

This section highlights some of the more direct implications of these case findings for the evaluation of conceptual frameworks, hypotheses, and research assumptions found in the research literature on the IT insider threat. For example, Wood (2002), noted that inside attackers are likely to target familiar domains and may even be domain experts. Our research supports this conclusion. In each case, the subject either attacked the system he was operating routinely or used this system to access the target of attack. The cases also include examples, such as the Attacker and the Time Bomber, of people who were experts with unparalleled technical and managerial authority over their systems.

Wood also assumed that inside attackers would be risk-averse and therefore likely to work alone, recruiting only trusted colleagues as allies. Schudel and Wood (1999) argued that a cyber-terrorist (presumably including insiders) would "prefer quiet, stealthy and passive techniques" and that this adversary's risk tolerance decreases over time as exposure or risk increases. While half of the 10 subjects in our study worked alone and nine out of 10 employed some form of operations security for their attacks, it might be a serious error to assume that these subjects were risk-averse beyond their operational planning. Their behavior both on and offline indicated that they were frequently disgruntled, emotionally aroused, and unable to avoid drawing attention to themselves.

As Table 6 indicated, eight of the 10 employees had personnel problems off-line, sufficient to merit official attention and intervention prior to their attacks. Several engaged in extremely risky online behaviors that drew attention to the likelihood of subsequent attacks. For example, the Saboteur ignored previous sanctions and made email threats to his supervisor. The Time Bomber also fought with his supervisor and unilaterally announced IT policies designed to facilitate his attack, while ignoring policies that interfered with his planning (such as the prohibition against taking corporate materials home).

Table 11 below shows our assessment of the rationality of each of the 10 subjects according to Wood's criteria of stealth, an emphasis on operational security, and general risk aversity. A subject was considered to have behaved rationally if he avoided drawing attention to himself or his issues prior to his attack, planned his attack versus acted impulsively, and included plans to protect himself from being identified as the attacker, consistent with his technical capabilities. A subject was not considered rational if he acted impulsively, drew attention to himself or his issues prior to the attack, and failed to plan his attack in a manner that he believed protected his identity. A subject who believed he was acting in a manner that would protect his identity but overestimated his abilities while underestimating those of his employer or investigators, was considered a rational actor.

Table 11
Review of Subject Rationality

Subject	Rational Actor	Non-Rational Actor
1. The Crasher		x
2. The Data Destroyer		x
3. The Hacker	x	
4. The Intruder		x
5. The Time Bomber	x	
6. The Extortionist	x	
7. The Saboteur		x
8. The Thief	x	
9. The Attacker		x
10. The Manipulator		x

As noted above, the Crasher, the Anonymous Intruder, the Saboteur and the Manipulator reportedly acted impulsively in the immediate context of a work setback. The Data Destroyer was also considered to have acted irrationally, including direct harassment of his love object in his attacks, which linked him directly to these efforts. The content of the Attacker's attacks, the fact that they occurred during bitter negotiations, and that he was the only one technically capable of these efforts also led to him being categorized as irrational. The Hacker, the Time Bomber, the Extortionist and the Thief appear to have acted after extensive planning but overestimated their deceptive skills due to personality traits affecting their judgment.

Table 11 also suggests a mix of risk-aversity among these subjects. The results support the need for caution in assuming that all insider offenders are risk-averse. This is particularly questionable if it supports a view of them as uniformly rational actors. Predictions of insider risk-aversion based on simulations of insider activity that utilize rational actor assumptions are likely to underestimate the threat posed by disgruntled employees.[6] It should also be noted that such individuals are prime candidates for recruitment by others, and frequently volunteer their services to competitors or adversarial interests, as the Thief case demonstrates. On the other hand, these cases also indicate that offenses by disgruntled insiders may be easier to detect, deter, and prevent than those of a more secretive rational actor.

In considering who would mount an insider attack, Wood gave only brief attention to individuals with character defects or from competitive organizations. Our results tend to bear out Wood's view that insiders tend to be loners, but also shed greater light on the specific characteristics of these individuals and especially their interaction within the workplace. The issue of subject characteristics and workplace interactions are considered in greater detail below. Wood also called for improved means of personnel

[6] Herbig and Wiskoff (2002) report that disgruntlement motivated 13% of espionage offenders having single motives; and for another 13% of offenders it was the primary motivations among multiple motives.

monitoring and reliability assessment—a recommendation supported by the data collected in these case studies.

Magklaros and Furnell (2002) proposed a probability-based tool for predicting insider misuse based largely on profiles of user behavior and anomaly detection. They noted the case of FBI Agent Robert Hanssen's abuse of his agency's Automated Case Support System in the act of espionage and argued that a system designed to detect this misuse would have warned of Hanssen's betrayal. Magklaros and Furnell have argued for automated software processes to detect risky behavior on operating systems, networks, and hardware. While this approach is widely utilized, the current data indicate some drawbacks. Our case studies indicate that some of the earliest predictors available of insider risk are noncomputer behaviors in the workplace. For several of our subjects, their attacks were the first online manifestation of their discontent. A software-based risk assessment system that concentrates only on computer-based behavior will, therefore, likely come late to the game. In addition, the more skilled and authoritative subjects in our cases disabled a considerable number of safeguards prior to their attacks and might be able to similarly deal with other proposed software countermeasures. A system that incorporated knowledge of offline risk—such as that posed by disgruntled employees—to raise its sensitivity to anomalies might be a more effective deterrent to insider threats.

Schultz (2002) addressed this problem in his expanded framework for predicting insider attacks. His proposed system calls attention to the need for diverse predictive indicators ranging from deliberate markers of threat preparation to verbal behavior and personality traits. The current research confirms the utility of several of his indicator categories including deliberate markers, preparatory behaviors (also noted by Wood), and verbal behavior. Schultz specifically notes the importance of email threats as an obvious indication that an attack is imminent.

A specific solution to the problem of capturing subject disgruntlement and incorporating it into a threat prediction system has been advanced by Shaw and Stroz (2004). Utilizing profiling methodology automated for risk assessment, we have recently produced and are testing software designed to detect changes in the emotional state and attitudes of individuals from their online communications, indicative of the emotions and attitudes associated with disgruntlement and risk of dangerous behaviors.[7] This patent-pending system is constructed to:

- Collect and analyze computer-generated and transmitted communications

[7]The psychological algorithms incorporated in the system were derived from psychological content analysis methods used in academic research, intelligence and forensic profiling (Shaw, 2001, 2003; Shaw et al., 1999). This approach would have captured the disgruntlement of several of the subjects considered, based on their email communications with their supervisors and colleagues. It also proved useful in the analysis of the Extortionist's correspondence with the FBI and in the analysis of the organization's communications with the subject as they attempted to control his anxiety and anger while luring him to a location where he could be arrested. Other examples of its application are included in Shaw and Stroz (2004), including illustrations with other insiders, such as Robert Hanssen.

- Utilize psychological profiling algorithms to evaluate the psychological state of the subject with special emphasis on detection of psychological states associated with threatening behaviors
- Use keyword algorithms to provide information on specific possible behaviors or actions the subject might take, as a result of this threatening psychological state
- Use communication-characteristic algorithms to assess possible targets of these potential threatening actions or behaviors
- Identify changes in the psychological state of a subject reflected in computerized communications that indicate an increased risk of potentially damaging actions
- Be programmed to draw the attention of qualified professionals and authorities to these detected changes in order to more fully evaluate risk potential and thereby increasing the ability of authorities to identify at-risk individuals based on large quantities of monitored computer-generated communications
- Be flexibly programmed to generate specific types of alerts or warnings and analysis depending on user requirements, including recommendations for user actions

Subject-Focused Research

Shaw (Shaw 2001, 2002; Shaw et al., 1998a, 1998b, 1999, 2000, 2001) proposed several hypotheses regarding characteristics of individuals at risk for insider acts and their interactions with the environment (or Critical Pathway) which led up to insider acts, and questioned whether it was possible to create a descriptive typology of potential insiders to aid in prediction and intervention. This section reviews the 10 cases in order to evaluate these hypotheses.

The Critical Pathway and At-Risk Characteristics

We believe that one of the most potentially valuable analytic frameworks for prevention advanced in previous research on insider attacks describes the *critical pathway* that is followed by many subjects on their way to committing insider violations (Shaw et al., 1998a, 1998b, 1999). The critical pathway shows how a subject's personal characteristics, personal and professional stressors, and interactions with others in the workplace could increase the risk of attack.

This pathway was defined as containing five interrelated components:

- The occurrence of significant personal and/or professional stressors within 6 months of the attack
- A maladaptive behavioral reaction to the stressor (which was hypothesized to be, in part, a result of a preexisting vulnerability to frustration, underlying anger at authority, poor social judgment and/or skills)
- An emotional reaction to the stressor

- The behavioral and/or emotional reactions in the workplace are sufficient to gain official attention (disciplinary action, counseling, etc.)
- The resulting managerial intervention is insufficient to divert the subject from the destructive pathway and may even escalate the process

This chain of the five hypothesized events is illustrated in Figure 2 below.

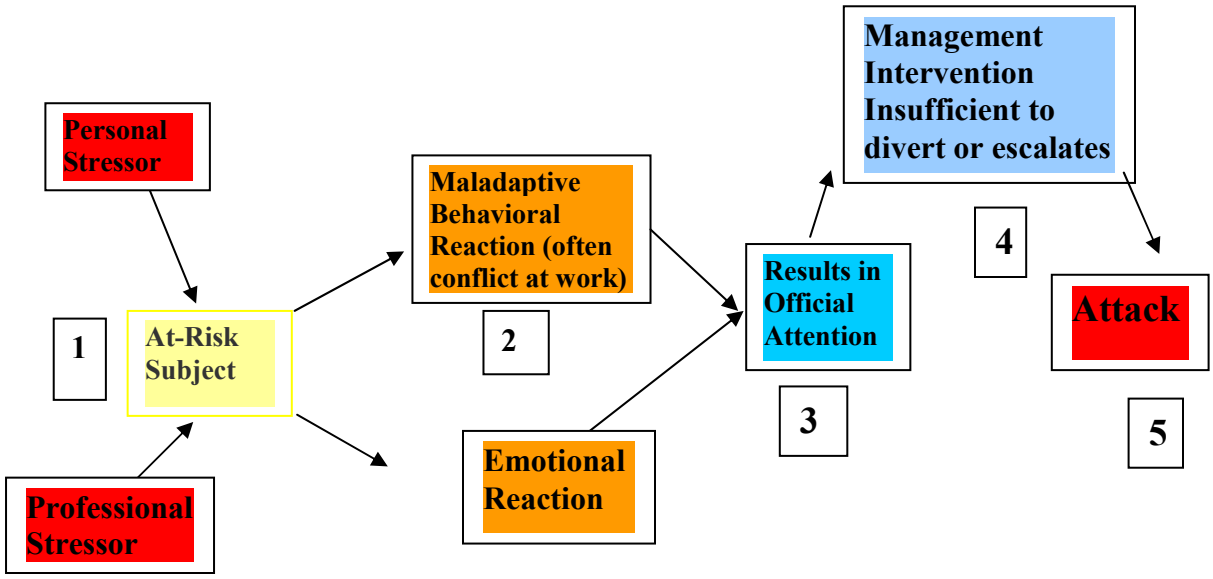

Figure 2 Events Along the Critical Pathway.

Data on the emotional reaction to the personal or professional stressors were also not available for three of the subjects in Cases 1–3. Case 3, the Hacker, is also slightly more complicated and different from the other eight cases because he was in the process of negotiating a deal with the owners/investors of his former employer, from which he was laid off. While his dismissal constituted a significant stressor and his decision to attack a potential client to prove the value of security services was poor judgment, his former employer saw no signs of emotional fallout left over from the earlier difficulties. The managing partner at this venture capital firm actually felt badly about the lay-offs and was trying to assist the Hacker and his colleagues at the time of the attack.

Table 12 examines eight of the case studies to determine whether the above pattern of characteristics and events was present. Cases 4 (the Intruder) and 6 (the Extortionist) were excluded from this review due to a lack of information.

Table 12
Critical Pathway Events

Pathway Event Subject	Personal/ Professional Stressors	Maladaptive Behavioral Reactions	Emotional Reactions	Official Attention	Ineffective Intervention
1. The Crasher	yes	yes	Unknown	yes	yes
2. The Data Destroyer	yes	yes	Unknown	yes	yes
3. The Hacker	yes	yes	Unknown	no	no
5. The Time Bomber	yes	yes	yes	yes	yes
7. The Saboteur	yes	yes	yes	yes	yes
8. The Thief	yes	yes	yes	yes	yes
9. The Attacker	yes	yes	yes	yes	yes
10. The Manipulator	yes	yes	yes	yes	yes

Examples of some of these steps on the pathway have been described in the context of discussions of case management, organizational change, and detection. These results also provide support to the observation offered by Gudaitis (1998) that "the vengeful inside intruder is actively sabotaging after they perceive their organization has done 'damage' to them."

In previous research on insiders who commit computer violations, Shaw et al. (1998a, 1998b) identified several characteristics that together may contribute to an increased risk of insider abuse. These characteristics may be summarized in four broad traits, including:

- *A history of negative social and personal experiences*: This history appears to manifest itself in a low threshold for frustration and a propensity for anger at peers and authority figures.
- *Lack of social skills and a propensity for social isolation*: Many subjects in the earlier studies appear to lack the social skills leading to an increased chance of success in school and social or professional settings. They appear to have turned to the computer and computer-based peer groups as a substitute for traditional social networks. Often the computer is used to mediate their social interactions at work. This lack of social skills tends to decrease the odds that when difficulties are encountered the subject will address these problems in a constructive manner. This combination of characteristics often leads the subject to express his grievances outside the organization to online contacts rather than through face-to-face, online or other direct contacts within the organization. His anger, frustration or disgruntlement then becomes visible through difficult personal interactions or emotional "leakage."
- *A sense of entitlement*: Many subjects appeared to behave as if they deserved special forms of attention and treatment such as exceptions to standard work policies and requirements. These feelings appeared to be derived from a sense that they possessed unique skills or gifts or that past difficulties merited compensation in the form of preferential treatment. This characteristic manifested itself in poor treatment of peers, difficulty adapting to social and professional requirements, and

a general need for unusual levels of attention from supervisors and peers. These subjects were often described as high maintenance.

- *Ethical flexibility*: Subjects in previous research appeared to lack the developed moral reasoning or attachment to others that would deter them from ethical violations. Researchers noted a lack of a conscience; lack of empathy for the harm they would be inflicting on others; and lack of loyalty to peers, supervisors, and the organizations affected by their actions. These characteristics were often associated with a failure to inhibit angry impulses and behaviors.

Figure 3 below illustrates how these characteristics may interact with the environment to increase risk in persons with these traits. The current research plan did not include the collection of extensive data on the personal development of these subjects or provisions for direct psychological assessments that would be best suited to determining the presence or absence of risk characteristics and their role in the violations described. However, limited information on personal history and current behaviors of the subjects has been gained from interviews with supervisors and coworkers, allowing the researchers to make some judgment as to whether the risk factors described above were present in each case. Table 13 indicates that clear evidence of these characteristics existed among eight cases.

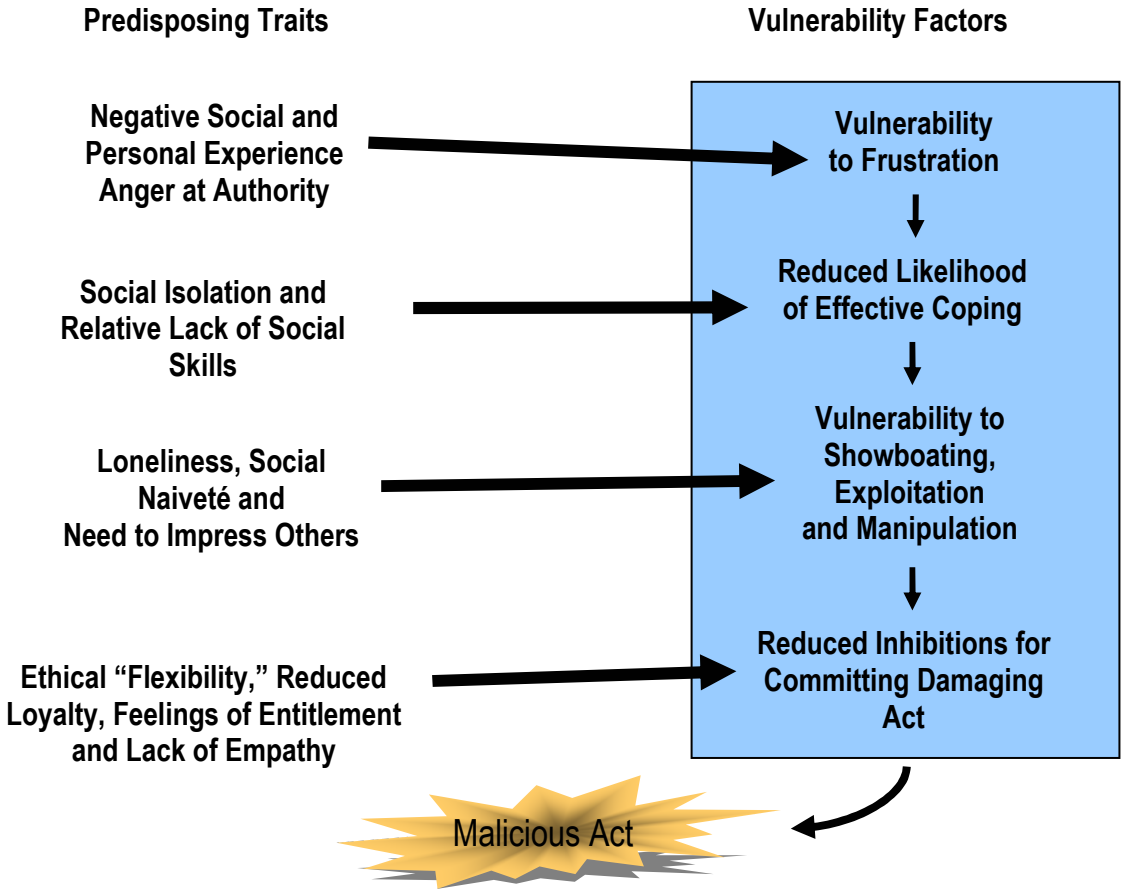

Figure 3 Effects of Personal Risk Factors in the Workplace.

Table 13
Distribution of Increased Risk Characteristics

Risk Characteristic Subject	Negative History	Lack of Social Skills	Sense of Entitlement	Ethical Flexibility
1. The Crasher	Unkn	Yes	Yes	Yes
2. The Data Destroyer	Yes	Yes	Yes	Yes
3. The Hacker	Yes	Yes	Yes	Yes
4. The Intruder	Unkn	Unkn	Unkn	Unkn
5. The Time Bomber	Yes	Yes	Yes	Yes
7. The Saboteur	Yes	Yes	Yes	Yes
8. The Thief	Yes	Yes	Yes	Yes
9. The Attacker	Yes	Yes	Yes	Yes
10. The Manipulator	Yes	Yes	Yes	Yes

These increased risk characteristics appear to have played a role in the subjects' progression down the critical pathway described earlier. For example, in his interview the Thief reported a long history of difficult international moves due to family financial stresses, being asked to leave his high school in this country and, just prior to his work problems, the divorce of his parents. He also reported significant frustrations in successfully completing the computer training necessary to become a network engineer. His frustrations in the workplace began to mount rapidly at his firm when he felt he did not receive the recognition he was entitled to for making important network engineering fixes. But rather than voicing his frustration to management, he withdrew and complained about these problems to his friends in the hacker community. The Thief's attitude problems and his inconsistencies at work led to his being placed on probation several months prior to the attack. At one point he wrote a lengthy memorandum on how managers must learn to handle hackers in the work environment differently than regular employees, indicating that he felt entitled to special treatment. For example, according to the Thief:

> "A hacker can be dramatically more effective than a nonhacker at a job, or dramatically less effective. Jobs where hackers are particularly good are: Systems administration, Programming, Design. Jobs where hackers are particularly bad are Data Entry. More generally, a job that requires fast and unexpected changes, significant skill, and is not very repetitive will be one a hacker will excel at. Repetitive, simple jobs are a waste of a good hacker, and will make your hacker bored and frustrated. No one works well bored and frustrated. The good news is, if you get a hacker on something he particularly likes, you will frequently see performance on the order of five to 10 times what a "normal" worker would produce. And yes, I am serious; a hacker on a roll may be able to produce, in a period of a few months, something that a small development group (say, 7–8 people) would have a hard time getting together over a year. He also may not. Your mileage will vary. IBM used to report that certain programmers might be as

> much as 100 times as productive as other workers, or more. This kind of thing happens."[8]

Confronted by what he felt was false advertising on the part of his company, the Thief felt obliged to correct the alleged misstatement by smuggling out the company's proprietary engineering plans to a hacker friend working for a competitor. He viewed this as getting the truth out and admits placing this value above loyalty or legal obligation to his company.

Another case illustrating this pattern involves the insurance company employee described in Case 2. This man's personal history included multiple arrests for forgery, grand larceny, and disorderly conduct. There were also court records covering complaints in landlord-tenant disputes and a protection order for harassment. Fellow employees described him as easily aroused, with a "bad temper." This employee also used his help desk position to make romantic overtures toward a female employee. He went so far as to create problems on her PC so that she would have to elicit his assistance. He repeatedly ignored and misinterpreted her statements of lack of romantic interest and, despite these rejections, escalated his pursuit. After further rebuffs, he reverted to harassment, significantly interfering with the female employee's work and personal life through her email communications. He denied accusations regarding these actions, even after being caught on video tampering with her computer. After his dismissal from the company, his acts of revenge escalated significantly, including unauthorized visits to the workplace and continued online sabotage.

Eight of the nine employees (excluding the Kazakh hacker the Extortionist) expressed their disgruntlement through interpersonal behavior off-line prior to reacting online. Only the Hacker reacted online and his attack appears to have been motivated by both anger and an effort to demonstrate the need for his security services. This finding emphasizes the need for close cooperation between human resource and computer security personnel.

Profiling the Insider Offender

Researchers studying espionage, a related manifestation of trust betrayal, have discounted efforts to profile offenders in favor of descriptive analysis. In a recent study of espionage trends, Herbig and Wiskoff (2002) state:

> "We contend that based on what we know from available data, there is not a "typical spy," and therefore there is no set of characteristics that could be used to "profile" a spy. This study does not try to produce a profile. Instead, the data presented in this study should lead to a better understanding of espionage. Espionage is a rare crime, and the most appropriate analytical approach to it is the use of simple descriptive statistics, i.e., frequencies of single variables and cross tabulations of several variables."

[8] Personal communication to the first author.

If efforts to profile IT insider offenders concentrate on development of single profiles designed to describe a typical offender, they are also likely to be as problematic. Admittedly, however, among IT insider offenders, there may be more in common among highly technical yet socially inept persons who are predisposed to insider technical attack than among the wide variety of recruited and volunteer espionage offenders. The typology that follows in Table 14 can be seen as a start in documenting not only attack behaviors of perpetrators, but also their emotional makeup.[9]

Table 14
Eight Perpetrator Subtypes

1. **Explorers:** curious individuals who commit violations in the process of learning or exploring the system, mostly without malicious intent; they are unaware that their activities violate company information-security policies (or such policies may not be in place).
2. **Samaritans**: individuals who bypass protocols and hack into a system to fix problems or accomplish assignments, believing their efforts to be more efficient than following approved procedures.
3. **Hackers**: individuals who have a prior history of hacking and continue penetrating systems after they are hired. These individuals have installed logic bombs or other devices in company systems to serve as job insurance when their activities are discovered. (They will defuse the trap in exchange for severance considerations.)
4. **Machiavellians**: individuals who engage in acts of sabotage, espionage or other forms of malicious activities to advance their careers or other personal agendas. They include those who steal intellectual property to become consultants, those who sabotage competitors (or superiors) and those who cause outages to facilitate their own advancement or ability to gain attention. Machiavellians may also use their skills to advance social agendas.
5. **Proprietors:** act as if they "own" the systems they are entrusted with and will do anything to protect their control and power over this territory. They may actively resist threats to their control and are willing to destroy or damage the system rather than give up control.
6. **Avengers**: classic disgruntled employees, who act impulsively out of revenge for perceived wrongs done to themselves.
7. **Career Thieves**: individuals who take employment with a company solely to commit theft, fraud, embezzlement or other illegal financial acts.
8. **Moles**: individuals who enter a company solely for the purpose of stealing trade secrets and other information assets for a competing company, outside group, or foreign country. (From Shaw et al., 2000)

A forensic profiler and leading authority on cyber-crime, Gudaitis (1998) voiced concern that security, management, human resource, or investigative personnel will substitute such "single profiles," predisposing traits, or case studies from previous incidents for deductive reasoning when trying to prevent insider attacks, or solve or

[9] An observation by Dr. Tom Longstaff of the Software Engineering Institute who reviewed an earlier version of this report before its release and offered many helpful suggestions.

mitigate insider cases. She rightfully rejects the direct substitution of these approaches for case-based profiling methods. She argues that the method of developing a single profile does not reflect the dynamic nature of individuals or the organizations in which they work. She also indicates that "true" profiling is not inductive or based on the compilation of past case studies, but deductive, based on the data available in the case at hand. She states, "Profiles are created on an individual, case by case basis."

It is difficult not to agree with Gudaitis's position that there is no single profile for inside attackers, although we are unaware of any research that has proposed such a silver bullet. It would also be a mistake to prioritize past research data or typologies over live, on-the-ground, case data when trying to prevent or solve insider cases. Such categories as predisposing traits or offender typologies can actually bias an investigative process if the profiler seeks to fit the data to the framework rather than remain open to the clues in the case. However, from this position, Gudaitis has, in effect, ruled out the use of past experience, data, and scientific research in profiling practice. While every case is different in many ways, the collection and analysis of case data and the assessment of similarities, differences and patterns across cases is basic to inductive scientific research. Even the best forensic profilers utilize past experience and patterns in their deductive processes. As Gudaitis noted, the FBI's Behavioral Science Unit's initial methodology was roughly defined as pattern recognition and it produced some important, empirically based profiling concepts such as the implications for perpetrator characteristics of an organized versus disorganized crime scene (Ressler et al., 1980). In this regard, Kaarbo and Beasley (1999) have discussed the use of empirical case study data as it contributes to and informs research and practice.

Gudaitis has observed that "the behavioral assessment tools used to prevent, predict, and mitigate incidents of computer crime are in their infancy (p. 338)." It is inconceivable that the growth of these approaches cannot be served by the application of basic scientific principles of hypothesis and theory-generation, data collection and hypothesis-testing. Empirically based theoretical research should inform applied profiling practice but no author is suggesting that it is a substitute for the deductive process. Other investigators are also pursuing this empirically based approach to criminal profiling to support the deductive process. These efforts by researchers like David Canter and Richard Kocsis were recently described by Winerman (2004).

When it comes to her own profiling analysis, Gudaitis reports adopting eight "theoretical" methodological constructs derived from traditional forensic practice. These include:

- *The victim*: In the case of computer crimes this would include the information system attacked and the peripheral victims impacted downstream such as the organization, employees, the community, and society at large.
- *The individual*: This concept includes every level of employee within the organization as well as the idea of the individual as a dynamic entity affected by their organizational, technological and social context. Risk within individuals increases as they become stressed by violations of their expectations. In addition,

the individual's expectations must be evaluated in conjunction with the expectations of the victim, the organization, and society.

- *Organization*: The nonhuman elements of a corporation such as its size, policies, structures, mission, business, rules and reinforcements. This category also includes "hot spots" or times within the organization when stress is normally increased.
- *Society and culture*: Everything outside the technology within a company, the individual and the organization. These components include the industry, clients and customers, competitors, current events, peers, and expectations.
- *Perpetrators*: Individuals who commit the crime, as well as unknowing individuals, the organization, the system and society, who may have facilitated the activity.

These five constructs are further assessed with respect to three other concepts:

- *Time*: Consideration of change, growth and decline in these factors over time.
- *Growth and decline*: The growth, development, or decline, regression or expiration of individuals, organizations, technologies and society over time.
- *Compatibility and conflict*: The mixing of technology, individuals, organizations and society over time and the manner in which they complement or conflict with one another.

Gudaitis calls for this method to be used in a qualitative fashion in a manner similar to anthropology, communication studies, criminology and semiotic psychology. While she would not support its use in this manner, her analytical approach overlaps significantly with the data collection scheme used in this research displayed in Table 2, including sensitivity to changes over time, conflict, and actor expectations.

Insider Offender Typologies

In previous research efforts were made to create subject typologies describing the motivation of offenders and their specific workplace behavioral presentations. Early efforts by Shaw et al. (1999, 2000) described a range of hypothesized subtypes with emphasis on their motivation for attacks, as shown in Table 15.

Subsequent efforts by Shaw (2001, 2002) attempted to expand the above typology beyond motivation to include the subject's behavioral presentation in the workplace, and relationships with peers and supervisors. Recent research has highlighted the relatively high frequency and serious threat posed by the Proprietor subtype (Shaw, 2001).

As shown in Table 15, 10 offenders in the current study can be categorized by perpetrator subtype according to case information available to researchers. As the table indicates, the subjects were equally divided between the Proprietor and Hacker categories, with two remaining subjects classified as Machiavellian/Avengers.

Table 15
Subject Typology Category

Case/Subject	Typology Category
1. The Crasher	Proprietor
2. The Programmer	Machiavellian/Avenger
3. The Hacker	Hacker
4. The Intruder	Machiavellian/Avenger
5. The Time Bomber	Proprietor
6. The Extortionist	Hacker
7. The Saboteur	Hacker
8. The Thief	Hacker
9. The Attacker	Proprietor
10. The Manipulator	Proprietor

Proprietors. The four Proprietors in this research behaved in characteristic ways, consistent with their efforts to retain control of their systems. This partial validation of the relevance of the Proprietor category, also allows further definition of the critical pathway—the channel "traveled" over time, described above, toward the attack—by subject type. For example, the Time Bomber case is paradigmatic of the Proprietor's pathway.

Like many Proprietors, the Time Bomber initially appeared to be a model employee. He was knowledgeable, dedicated and responsive to management needs. Compared to other staff, he is on the cutting edge of a new technology, facilitating group dependence on his skills. However, with this success, he began to operate as if he had personal control and ownership of the company's computer system. He successfully cultivated supportive relationships with senior employees to protect his turf. He successfully resisted manager efforts to dilute or curtail his computer policies and control of the system. He specifically refused orders to train backup personnel, including his supervisor. He appears to have been willing to destroy the system and damage the company rather than give-up control. Like other Proprietors, he used his unique system knowledge to construct a long-term strategy to disable the system, if necessary, to protect his interest or position in the company.

Ultimately, his control over the system also facilitated unique operational security for his plans, including the opportunity for multiple rehearsals of his attack. His attack coincided closely with his termination—his loss of control of the system— as in other Proprietor cases. Finally, he appears to have valued control over the system above his own self-interest as the attack was readily traced to his activities. This level of irrational thinking is typical of Proprietors whose unique position often leads them to overestimate their own abilities and under-estimate the abilities of others. This may have been the case with the Time Bomber in whose plan to use the attack to rejoin the company as a consultant, underestimated the extent and thoroughness of the firm's reaction. As more cases of proprietor abuse emerge the validity of this specific pathway model will be tested. It is our expectation that the range in personality characteristics, motives,

workplace interactions and other factors will result in different critical pathways or narratives by subtype.

Hackers. The relatively high frequency of Hackers in this selection of cases was surprising. However, when the three insider hackers (the Hacker, the Saboteur and the Thief) are examined there are notable similarities in their pathways to the attack. These included:

- A significantly adverse personal history. The Saboteur and the Hacker had criminal records and the Thief had been expelled from high school and had a history of hacking activity
- A history of previous computer misuse
- On or shortly after the date of their employment, disabling of organizational security devices
- Disregard for security and personnel protocols
- Significant self-esteem issues that require unusual attention, making the subject sensitive to slights or generally a high maintenance employee
- Personnel conflicts or problems requiring official attention
- An angry reaction to a company policy or action related to him or his interests
- A lack of inhibitions about retaliation or revenge for these perceived activities

The case of the Saboteur particularly fits the Hacker subtype described in earlier research. His criminal background is consistent with other hackers studied in this sample, including his history of previous computer misuse and drug offenses. Like other hackers studied, he set up a system to assure operations security upon his arrival. This reportedly included the elimination of the history logs and the activation of sniffers to gain access to his supervisor's files. For example, he knew about his termination letter when it was in draft form on his supervisor's password-protected email program. His hacking skills also made him immune to normal security controls and sanctions. He also demanded and received exceptional treatment due to his technical skills, ignored security policies and procedures, and actively fought security interventions designed to curtail his access.

The Saboteur also made unilateral changes to system configurations without prior approval; these resulted in system disruptions. When he was finally threatened with termination he countered by attacking the system. His personality characteristics (narcissism and sociopathy) and interpersonal behaviors (arrogance, propensity for conflict with others, resistance to authority, and disregard for policies and practices) were also consistent with those of his hacker peers. Also classified as a hacker, the Extortionist differed from the other subjects in this category in several ways. He was not a direct insider, but had access to his target through his organization's subscription. He was also not a disgruntled employee but rather more of a calculating criminal who wanted to use his familiarity with the targeted system and his computer skills for financial and employment gains. To this end he worked closely with an attorney, translator and another accomplice to execute a now common extortion plan.

Table 16 presents an overview of some of the characteristics of these hacker subjects, including ratings by investigators. Of interest for screening, only half have criminal records. They are not loners, as three out of four acted with others to attack their systems. While they are affiliated with the hacker community, they have varying degrees of status within this subculture.

Table 16
Overview of Hacker Subjects

Subject	Age	Tech Capability	Prior Legal Issues	Acted with Others	Status in Hacker Community
3. The Hacker	29	High	Yes	Yes	High
6. The Extortionist	30	High	No	Yes	Unknown
7. The Saboteur	20	High	Yes	No	Low
8. The Thief	23	Low	No	Yes	Low

Machiavellian/Avengers

The two cases described above as combination Machiavellian/Avengers speak to the difficulty of establishing subject motivation. It is difficult to isolate or eliminate revenge as a motive in cases involving disgruntled employees. The lack of mutual exclusivity of the Avenger subtype indicates a need to refine this motivational category in future research.

The insurance company employee described in Case 2 was classified as a Machiavellian turned Avenger because he used his IT skills to pursue a romantic target and to attempt to control and punish her for negative responses. His attacks on his former organization's payroll system appeared to be exclusively related to this interaction and in revenge for his termination for his behavior.

In the case of the Intruder, interview results with the subject led to his classification as someone taking intellectual property that he thought was his, out of concern for his future career, while interviews with his former employers tended to characterize him as an Avenger seeking to harm his former company. They feared he was stealing a proprietary client database to both advance his career and seek revenge for his abrupt termination. We cannot be certain whether this was his intent but his employers sought and won an injunction against his transferring or making use of this data.

Conclusions and Lessons Learned

The above patterns, though based on only 10 cases, have implications for policies and practices related to insider prevention, detection, management and investigation. They can also be used to facilitate further insider research and produce security education materials. Work currently being undertaken by PERSEREC, the FBI Academy's Behavioral Sciences Unit and by the U.S. Secret Service in collaboration with the

Software Engineering Institute may validate, extend or qualify conclusions and observations from the present study.

Prevention

The diverse personal and professional characteristics of the subjects studied indicate that disgruntled insiders can come from anywhere within the IT organization. Our subjects included help desk staff, programmers, system administrators, division heads, and a Chief Technical Officer (CTO). The broad distribution of their positions within their organizations, time on the job, age, marital status, and other variables make the formulation of an at-risk profile based on demographic features extremely difficult if not impossible. However, there are some common or frequently observed patterns that may signal elevated vulnerability in future situations. For example, nine out of 10 of our subjects were in the process of dealing with an extremely serious employment problem that had ended or threatened their jobs. Most of these conflicts arose during the third and fourth quarters of their tenure.

Other indicators of vulnerability that might have led to detection included the occurrence of significant organization-wide changes or stresses as well as personal stressors affecting the employee. Another marker of risk was the unique level of system access and/or control obtained by many of these subjects—sufficient to make their managers feel intimidated and threatened in their dealings with these subjects. Finally, these individuals were consistently engaged in social or cultural work place conflicts. Table 17 summarizes these key findings and implications relevant to prevention.

Detection

Table 18 summarizes key findings and implications relevant to detection or intervention during periods of elevated risk. The fact that nine of the subjects employed methods to hide their activities complicated prospects for insider detection by electronic methods. This is especially true when the unique technical skills and positions of the subjects are considered. It is also a strong argument for the use of improved and independent system monitoring capabilities. Regular outside audits by independent computer security firms utilizing passive monitoring systems might address the use of covert methods and security protocol violations by technically skilled subjects or subjects with authority over IT operations.

Combined with the strong finding above that nine of the 10 subjects were engaged in serious employment crises, this finding on the use of operations security to hide their system abuse reinforces the high value of personnel problems as a predictor of insider risk. This conclusion was further reinforced by findings on the occurrence in nearly every case studied of subject disgruntlement and serious personnel problems months prior to an attack. These subjects reacted to off-line personal conflicts, stresses, and disappointments through electronic behavior. The data from these subjects also indicated that the post-termination window for an attack can range from hours to up to 2 months. One of the most important findings of this research was that there was a window of opportunity for

Table 17
Key Findings and Implications Relevant to Prevention

Key Findings: Risk Factors Contributing to Heightened System Vulnerability	Implications Related to Prevention of Attacks
Diverse location of subjects within the IT organization	1. Need for broadly based prevention and detection programs.
Presence of very serious subject employment problems	2. Need for improved and more aggressive management of at-risk employees undergoing personnel problems with greater emphasis on security risks.
Organizational stress as risk indicator	3. Advisability of increasing alert and monitoring levels during periods of stressful organizational change, improving and increasing stress interventions for employees.
Intimidation of manager by offending IT professionals through their control of the system and influence in the firm	4. Improved management training, enforcement of basic security precautions against over-dependence on subjects (two-man rule, etc.).
Problems with probation and termination processes	5. Need for revised probation and termination procedures to decrease vulnerability to attacks, reduce likelihood of attacks during these periods and to monitor attack risk more effectively.

Table 18
Key Findings and Implications Related to Detection

Key Findings: Indicators of Impending Attack on the System	Implication Related to Detection or Intervention During Periods of Elevated Risk
Use of OPSEC by the subject	6. Need for regular outside audits and increased use of personnel versus electronic indicators of risk, increased sensitivity to the expression of interpersonal disgruntlement in online formats.
Occurrence of personnel problems prior to electronic attacks	7. Need for improved detection and management of personnel problems, improved communications between personnel and computer security staff, improved policies and procedures, awareness training, integrating management of personnel problems and computer security, advisability of integrating detection of disgruntlement into computer monitoring systems.
High frequency of post-termination attacks	8. Need for improvement in management and security of the termination process and post-termination monitoring of at-risk employees.
Personal stress as risk indicator	9. Advisability of increasing alert and monitoring levels during periods of personal stress in at-risk subjects, more aggressive personnel interventions.
Social and cultural conflicts as risk indicators	10. Advisability of increasing alert and monitoring levels during social and cultural conflicts, intervening aggressively to reduce employee stress.
Window of opportunity to intervene prior to attacks	11. Improved manager, personnel and security training regarding the risk of personnel problems, need for aggressive detection and intervention and effective interventions to reduce risk.
Subjects' use of remote access for post-termination attacks	12. Need to revise remote access policies and practices, especially after detection of subject risk and during probation and termination periods.

dealing with the personnel problems affecting these subjects. These individuals were reportedly disgruntled in some cases for over a year prior to their attacks, and management was aware of these personnel problems weeks, if not months, prior to the attack. Yet there were consistent intervention problems. In fact, in many cases ill-considered management actions exacerbated the problem. This finding indicates the need for improved management training and procedures covering interventions with at-risk individuals.

There were also several problems with the probation and termination processes in these cases. Most notably, after the employee had left the work site due to termination or probation, there was a failure to block his access to the system, facilitating the high rate of remote attacks. Nor was the access by employees on probation remaining on site effectively curtailed or monitored. The high rate of post-termination attacks indicates the need for a careful review of personnel and security issues prior to the termination of at-risk employees. In addition, it may be beneficial to reexamine policies and practices related to remote access. While remote access can increase productivity, organizations may need safeguards (such as the right to on-site inspection) to ensure that this access is not abused, especially following termination. A medical institution that recently received recognition for its security training tactics reports revoking remote access rights after any episode of noncompliance with IT security practices (Briney, 2003).

These findings strongly reinforce the need for more thorough and aggressive investigation of disgruntled IT employees from a risk perspective. Such inquiries should involve both a psychological (actual versus perceived sources of disgruntlement, level of dangerousness, type and timing of risk) and security (access, skills, possible MO, likely vulnerabilities, countermeasures) perspective.

Personnel Management

The high rate of gaps in employment and security policies in these cases that either led to insider activity or failed to help prevent or detect it indicate the need for more widespread security policy education and threat awareness in national infrastructure industries. The fact that there were even higher rates of policy implementation and enforcement failures suggests the existence of an even deeper problem. In many of these cases involving implementation and enforcement failures, technical means were not present to enforce the policy, human resources were lacking, personnel did not understand the importance of the policy, or the offenders simply utilized superior system knowledge to ignore and evade enforcement efforts.

The failure to screen these subjects prior to their admission to the worksite was the most significant finding related to prevention and vulnerability. In addition, many of the subjects gained employment through family channels, which may have reduced (in these specific cases) the employer's perception of the importance of more formal background checks. While several of the subjects had previous criminal convictions that would have been discoverable during a background check, others had hacker affiliations that might have been overlooked by standard reviews. This finding indicates the need for

the expansion of standard pre-employment screening to detect this type of risk. The finding that several subjects had either committed the same or similar crimes before, or went on to repeat their violations, calls attention on the need for a system to track IT offenders better. Table 19 below summarizes these key findings and implications related to personnel management and insider risk.

Table 19
Key Findings and Implications Related to Personnel Management

Key Findings: Risk Factors Related to Personnel Management and Policy that Predict to Greater Vulnerability	Implications Related to Personnel Management and Policy
Gaps in personnel and security policies and practices	13. Need for increased education and proliferation of personnel and security policies and practices, audits of policies and practices.
High rates of personnel and security policy implementation and enforcement failures	14. Need for increased education and proliferation of personnel and security policy implementation and enforcement methods, management training in enforcement practices, case management training, more reliable consequences for violations.
Lack of technical and human resources and education for policy enforcement	15. Improved education and awareness training regarding policy enforcement, improved enforcement auditing, increased corporate self-regulation of policy enforcement to avoid liability, government regulation and legislation.
Offender ability to avoid detection of policy and practice violations	16. Improved education and training of personnel and security personnel responsible for policy implementation and enforcement, and improved technical and human resources to assist these personnel.
Failure of basic screening procedures	17. Need to increase screening requirements.
Failure of traditional screening methods to detect at-risk online activities	18. Need to broaden and improve screening to improve detection of hacking and other at-risk, online activities and affiliations, use of security audits early in employment in absence of reliable screening methods.
Tracking failures	19. Need to improve availability of information regarding past prosecuted and nonprosecuted violations for pre-employment screening.

Criminal and Incident Investigations

The patterns observed across these cases can potentially aid investigators of insider activity. While there may not be an insider "personality profile" to facilitate investigation, there are clear patterns in the combined personal backgrounds and work relationships that make these individuals stand out among their peers. The Proprietor and the Hacker perpetrator types provide even more detail on potential suspect characteristics. When partial information on suspects is available that fits these templates, they can provide further investigative guidance. The combination of personal characteristics and

problematic interactions in the workplace, identified in these case studies as risk indicators, could help narrow a field of suspects or assist investigators and prosecutors to select appropriate case management strategies.

Future Research

These results provided tentative support for the validity of the critical pathway model and the accompanying at-risk characteristics. The findings also lend support to the accuracy and relevance of the perpetrator typology categories. It would be useful to compare the patterns associated with the critical pathway and the perpetrator typologies to subjects in other types of trust betrayal, including insider espionage, fraud, and support for terrorist organizations.

The research approach could be significantly improved in several ways. An increase in the frequency of subject interviews would fill out the story of these events and provide critical information on the relative balance of individual versus organizational factors that contribute to these episodes. However, these results indicate that subject interviews alone— without workplace and investigator information and coworker interviews—may result in a significant social desirability bias. The three subjects in this sample who agreed to interviews had very specific agendas for doing so. In these cases subject interviews were balanced by alternative views of the event provided by coworkers and supervisors which in many cases conflicted with those of the subject. The availability of alternate sources provided a deeper understanding of the motivations and behaviors associated with each event.

- The number of and variety of subjects available could be increased easily by expanding the geographic selection area beyond the Washington, DC, to the New York corridor.
- The research could be further improved by diversifying selection to include cases not handled by law enforcement. The absence of court findings would require strengthening of the criteria to validate the nature of the offense. These preliminary results suggest that there may be differences between criminal cases and those more numerous violations resolved without legal intervention.
- Expansion of the number of subjects would also allow for more robust data analysis, beyond the examination of trends.

Educational Products

Detailed case studies provide unique educational value. The level of human detail, the focus on seemingly normal workplace events, and the application of critical pathway analysis, can be used to sensitize peers, supervisors, and security personnel to insider risks and intervention opportunities.

Potential educational and training opportunities and products derived from this research could include:

- Live or taped interviews with subjects, investigators, coworkers and prosecutors from a specific case
- Classroom exercises written around actual case data that would allow participants to role-play interventions at different stages of a case as the risk of an insider attack increases over time
- Structured security and investigative class work utilizing the case patterns identified to help security personnel refine investigative strategies
- Improved red teaming[10] from the insider perspective
- Materials designed to help security personnel work more closely with Human Resources and employee assistance program staff to identify and appropriately intervene with employees at risk for insider activity
- Information designed to help security and counterintelligence personnel prioritize scarce resources to identify groups, as well as individuals, at-risk for insider activity.

Summary

The foregoing 19 specific findings and implications reflect a more limited set of central observations derived from these cases. The following can be considered the primary conclusions and lessons learned from this study that have obvious application to cases like those described here for personnel policy, personnel security practices, technical deterrents, and security education for employee populations.

1. There is a clear relationship between personal stress as well as adverse social climates and the level of risk for systems abuse. Reliance on software solutions or technical deterrents to cyber-crime tends to obscure the importance of addressing personal issues through management interventions and timely referrals to employee assistance programs when appropriate. What is going on in a trusted employee's life (whether it be threatened loss of employment, marital strife, or substance abuse) usually manifests itself in workplace behavior and attitudes. When that person is in control of an IT system, the risk is even greater.

2. Closely related to the above is the policy issue on how to deal with disgruntled employees who have access to critical information system. Most of the offenders in these case studies were disgruntled for one reason or another. They reacted to their perceptions of injustice by abusive online behavior. An employee who is expressing anger in the workplace is engaged in conflict with other employees, or otherwise behaving in a threatening manner needs immediate management intervention. Our cases, albeit limited in number, indicate that there is a time delay in management awareness of employee disgruntlement and therefore a limited window of opportunity for more effective management responsiveness to this challenge. In addition, our limited sample raises

[10] Red teaming is a strategy for the testing of network defenses against intrusion or attack. A team of technical experts, given authorization to do so, attempts to break into a system from a remote location as would a group of hackers.

questions about the effectiveness of many management approaches once an intervention is attempted. These results and the high-risk levels in such situations argue for the establishment of strict human resources guidelines regarding reporting and intervention with such subjects. These results indicate the need to consider more intensive, multidisciplinary case management and planning, as well as such options as intensive monitoring, restriction on remote system access, counseling, or psychological evaluation to mitigate the threat of systems abuse by employees at risk.

3. Even where disgruntlement or stress are not factors, these cases indicate that an elevated vulnerability to abuse exists in organizations that permit systems administrators or other IT professionals exclusive or proprietary control over its information systems. Where the system administrator has a sense of ownership and possesses technical skills not shared by other members of the organization, a situation exists in which management has no supervisory oversight and may well be intimidated by the administrator. The solution to this vulnerability is to require some type of routine system audit or monitoring by an independent provider or shared responsibilities for IT functions within the organization by technically qualified persons.

4. Inadequate termination policies appear to have been a contributing factor in several cases studied here and in other insider events evaluated by the research team. Where termination of employment or temporary probation appears to be a necessary action in extreme cases, the organization must protect itself and its systems from acts of retribution. Immediate suspension of system access (remote and on site) as well as physical access to the workplace by a terminated employee may be warranted, particularly when that employee has had some level of functional control of the IT system.

5. While remote access to a critical information system can be justified as a convenience or as a necessity stemming from mission requirements, experience indicates that unmonitored remote access carries intensified risks to an IT system. System vulnerability is heightened by not suspending remote access privileges of an employee who is barred from the workplace, known to be disgruntled, or who has a history of disregarding security rules and procedures.

6. It is clear that some of the system abuse reported in these cases would not have occurred had there been effective pre-employment screening of job applicants, particularly in regard to past history of online and criminal behavior. Employers, whether in government or the private sector, face serious risks by hiring IT professionals based simply on personal recommendation or paper credentials. However, several of these cases indicate the inadequacy of standard background checks for detection of prior activities of concern which were not prosecuted or not part of the public record—for example, hacker activity. This screening gap and the quickness with which several of these subjects violated information security protocols upon their arrival in the workplace argue for probationary audits of the computer activity of new IT employees.

7. A review of these cases in the private sector and of insider cyber-crime and abuse in DoD organizations shows that some of these damaging events could have been avoided by adequate security training, education, and awareness for employees having access to, or control over, critical information systems. Educational and awareness programs for the workforce and the timing of awareness communications may be geared to activate during periods of higher vulnerability for the organization or during a window of opportunity after signs of employee disgruntlement surface.

8. In some of these cases, the failure to alert management to at-risk subject behaviors can be attributed to gaps in security policy. Also seen was inadequate enforcement and follow-up to policy violations due to a lack of resources or personnel training. Several subjects were simply able to evade security policies because they had IT skills superior to those responsible for enforcement. The content of education and training to address these gaps should include not only technical vulnerabilities but also security policies, deterrent measures, coworker responsibilities, and consequences for systems and for offending employees resulting from insider abuse. The use of actual case studies such as those described in these companion reports can enhance the effectiveness of these educational efforts.

References

Academy jurors get lesson in hacking during cadet's trial. (1999, March 16). *Colorado Springs Gazette Telegraph*.

Air Force Academy dismisses cadet for hacking into computer. (1999, March 14). *Chicago Tribune*, p. 18.

Briney, A. (2003). Best training tactics. *Information Security, 6*(12), 45.

Burgess, A.W., Hartman, C.R., Ressler, R.K., Douglas, J.E., & McCormack, A. (1986). Sexual homicide: A motivational model. *Journal of Interpersonal Violence, 1*(3), 251–272.

Caruso, V.L. (2003). *Outsourcing information technology and the insider threat*. Unpublished master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH.

Coast Guard beefs up security after hack. (1998, July 20). *Computer World*.

Fischer, L.F. (2003). Characterizing information systems insider offenders. *Proceedings of the 45th Annual Conference of the International Military Testing Association*, Pensacola, FL. Retrieved, 2003, http://www.internationalmta.org

Gudaitis, T. (1998). The missing link in information security: Three-dimensional profiling. *CyberPsychology and Behavior*, *1*(4), 321–340.

Herbig, K.L., & Wiskoff, M.F. (2002). *Espionage against the United States by American citizens 1947–2001*. Monterey CA: Defense Personnel Security Research Center.

Kaarbo, J., & Beasley, R. (1999). A practical guide to the comparative case study method in political psychology. *Political Psychology, 20*(2), 369–391.

MSNBC. (2000, May 1). Stiff penalties sought for computer crime. Retrieved May 1, 2000, from http://zdnet.com/2100–11–520372html

Magklaros, G.B., & Furnell, S.M. (2002). Insider threat prediction tool: Evaluating the misuse. *Computers and Security, 21*(1), 62–73.

Ressler, R., Burgess, A.W., & Douglas, J.E. (1980). Sexual homicide: Patterns and motives. *FBI Law Enforcement Journal*, *49*(10), 16–20.

Schudel, G., & Wood, B. (1999). Modeling behavior of the cyber-terrorist. *Proceedings from Countering Cyberterrorism Workshop*. Marina del Rey, CA: University of Southern California, Information Sciences Institute. Retrieved December, 2004, from http://www.isi.edu/cctws

Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security, 210,* 526–531.

Shannon, E., & Blackman, A. (2002). *The spy next door: The extraordinary secret life of Robert Philip Hanssen, the most damaging FBI agent in U.S. history*. New York: Little, Brown.

Shaw, E.D. (2001, January). To fire or not to fire. *Information Security*, 48–57.

Shaw, E.D. (2002). *Profiling corporate information technology insider risk*. Washington, DC: Consulting & Clinical Psychology.

Shaw, E.D. (2003). Saddam Hussein: Political psychological profiling results relevant to his possession, use and possible transfer of weapons of mass destruction (WMD) to terrorist groups. *Studies in Conflict and Terrorism*, *26*, 347–364.

Shaw, E.D. (2004). The insider threat: Can it be managed? In Parker, T. (Ed.), *Adversary characterization*: *Auditing the hacker mind.* Rockland, MA: Syngress Publications.

Shaw, E.D., Ruby, K.G., & Post, J.M. (1998a). *Insider threats to critical information systems: Characteristics of the vulnerable critical information technology insider (CITI)* (Tech. Rep. No. 2). Bethesda, MD: Political Psychology Associates.

Shaw, E.D., Ruby, K.G., & Post, J.M. (1998b). The insider threat to information systems. *Security Awareness Bulletin*, 2–98, 27–47.

Shaw, E.D., Post, J.M., & Ruby, K.G. (1999, December). Inside the mind of the insider. *Security Management,* 34–44.

Shaw, E.D., Post, J.M., & Ruby, K.G. (2000, July). Managing the threat from within: The personnel security audit. *Information Security*, 62–72.

Shaw, E.D., & Stroz, E. (2004). WarmTouch software: The IDS of psychology. In Parker, T. (Ed.), *Adversary characterization: Auditing the hacker mind.* Rockland, MA: Syngress Publications.

Shaw, E.D., & Fischer, L.F. (2005). *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders; Report 2, case studies.* (FOUO) Monterey, CA: Defense Personnel Security Research Center.

Winerman, L. (2004). Criminal profiling: The reality behind the myth. *Monitor On Psychology, 35*(7), 66–69.

Woman gets five months for hacking; tampering ruined Coast Guard files (1998, June 20). *The Washington Post.*

Wood, B.J. (2000). *An insider threat model for adversary simulation*. Menlo Park, CA: SRI International, Cyber Defense Research Center.

Wood, S., & Fischer, L.F. (2002). *Cleared DoD employees at risk – Report 2. A study of barriers to seeking help.* Monterey, CA: Defense Personnel Security Research Center.